(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 March 2003 (06.03.2003)

PCT

(10) International Publication Number
WO 03/019459 A2

(51) International Patent Classification⁷: G06K

(21) International Application Number: PCT/US02/26617

(22) International Filing Date: 22 August 2002 (22.08.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/314,926	24 August 2001 (24.08.2001)	US
10/164,070	6 June 2002 (06.06.2002)	US

(71) Applicant: ZEBRA INVESTMENT HOLDING CORPORATION [US/US]; 1201 Market Street, Wilmington, DE 19801 (US).

(72) Inventors: HOHBERGER, Clive, P.; 630 Vernon Avenue, #5, Glencoe, IL 60022 (US). TSIRLINE, Boris, Y.; 4561 W. Westchester Lane, Libertyville, IL 60048-4877 (US).

(74) Agents: COHEN, Eric, D. et al.; Welsh & Katz, Ltd., 120 South Riverside Plaza, 22nd Floor, Chicago, IL 60606 (US).

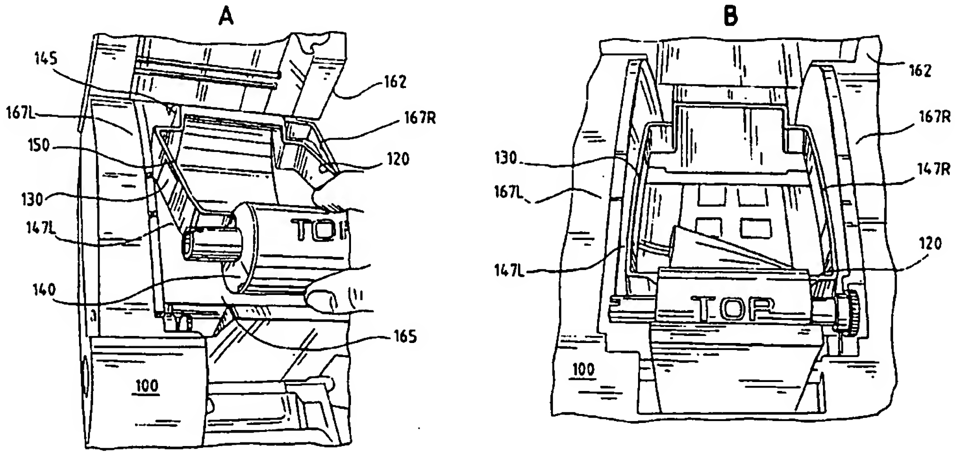
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND APPARATUS FOR ARTICLE AUTHENTICATION



(57) Abstract: An authentication method for authenticating an article in a device includes the steps of a) reading an identification number stored on the article, b) reading an authentication number stored on the article, c) determining an input number based at least in part on the identification number, d) applying an authentication function to the input number to calculate an output number, e) determining that the article is authentic only if the authentication number corresponds to the output number, and f) permitting use of the article in the device if the article is authentic, and disabling use of the article in the device if the article is not authentic.

WO 03/019459 A2

METHOD AND APPARATUS FOR ARTICLE AUTHENTICATION

This invention relates generally to an authentication technique for an article used in a host device. More specifically, one particular embodiment of this invention relates to an improvement to an ink cassette or cartridge in a thermal marking apparatus wherein the ink cassette or ribbon cartridge may be authenticate as being of a suitable type and coming from an authorized source.

BACKGROUND

Other approaches have been tried for authenticating consumables in a host, but none of these have proven satisfactory. In particular, the background approaches discussed below do not provide an effective anti-piracy deterrent. These previously known approaches do not provide adequate authentication and can often be defeated by copying, spoofing, or similar techniques.

One early technique to authenticate consumables relied on keyed shapes of the consumable. Such keyed shapes can be designed so that only a consumable in the keyed shape will fit into a given type of host. As one example, a particular brand of razor can be adapted to receive only razor blades having a particular keyed shape. As a second example, an ink jet printer can be adapted to receive only refill ink cartridges having a particular keyed shape. The use of such a keyed shape can prevent interchange of consumables between different types of host. That approach is generally ineffective for anti-piracy, however, because the keyed shape of the consumable can be readily observed and easily duplicated.

Also unsatisfactory are the "challenge and response" authentication algorithms used in transponders intended for automobile security systems, such as the Atmel TK556, and equivalents. Automotive security systems were designed for "one lock, few keys" applications, where a single secret number is programmed into each key and each lock. If a host device, such as a printer or a camera, is the "lock," then such challenge-response transponders require that all the keys (media) and locks (printers) be programmed with the same secret number.

It is known to provide encodements on consumables, such as film units and/or hosts such as cameras, for identification purposes and to convey information about the film unit or camera. The term "encodement" very broadly describes a feature of physical media used to communicate one or more pieces of information to a machine. "Encodement" includes alphanumeric text and other indicia, symbols, and the like. An encodement can be detectable by various means, including but not limited to optical, magnetic, and/or punch readers.

U.S. Patent No. 6,106,166 discloses a device having a transponder and a transceiver. An electrically or electronically programmable read/write memory contained in the transponder is integrally attached to a consumable. The transponder is capable of receiving a first RF frequency electromagnetic field and deriving power and address information therefrom, and then generating a second RF frequency electromagnetic field in response. The second electromagnetic field is characteristic of the data stored in memory. A transceiver is disposed within the host with an antenna and support components for polling each transponder. As instructed by a control logic processor, the transceiver can read manufacturing data from the transponder and write usage and processing data to the transponder for storage in memory.

Radio-frequency identification transponders are widely available in a variety of forms. One form, referred to as "inlay transponders" are identification transponders that have a substantially flat shape. The antenna for an inlay transponder is in the form of a conductive trace deposited on a non-conductive support. The antenna may have the shape of a flat coil and the like. Leads for the antenna are also deposited, with non-conductive layers interposed as necessary. Memory components, RF communications, and any control functions are provided by a chip mounted on the support and operatively connected through the leads to the antenna. Inlay transponders have been used as layers of identification tags and labels to provide encodements that are accessible at a distance. A camera having a radio-frequency identification transponder that can be accessed for writing and reading at a distance is disclosed in U.S. Patent No. 6,173,119.

Another known type of transponder is a radio frequency identification (RFID) transponder. An RFID transponder can typically include a unique identifier installed by the manufacturer in non-volatile memory.

With respect to host devices, it is known to provide a consumable article, such as a print cartridge, with a transponder. The host device, such as a printer into which the cartridge is installed, includes a transceiver for detecting the type of media on the print cartridge. A transceiver and transponder of this general type are disclosed in U.S. Patent No. 6,099,178 to Spurr et al. The Spurr patent discloses a printer adapted to sense the type of media installed and includes a radio frequency transceiver for transmitting a first electromagnetic field, and for sensing a second electromagnetic field. However, Spurr does not teach or suggest a means for authenticating the media bearing the transponder. The information encoded in the transponder in Spurr can be easily forged, thus rendering the system ineffective as an anti-piracy measure.

International Publication Number WO 98/52762 discloses an inkjet printer that uses an RFID tag for identifying the type of paper that is loaded in an inkjet printer. That approach offers contactless communication with a read/write memory that is added to the inkjet roll. That publication, however, does not teach or suggest an authentication method and apparatus in accord with this disclosure.

A need exists, therefore, for an effective anti-piracy measure using a transponder and transceiver for sensing information encoded on a consumable article for use in a host device, such as media for use in a printer.

BRIEF DESCRIPTION OF THE DRAWINGS

It is believed that the invention will be better understood from the following description when taken in conjunction with the accompanying drawings, wherein:

FIG. 1A is a top left perspective view of a consumable article being loaded into a host device in accordance with one embodiment.

FIG. 1B is a top front perspective view of a consumable article loaded into a host device in accordance with one embodiment.

FIG. 2A is a program flowchart depicting one embodiment of a sequence of operations to prepare an authenticatable consumable article.

FIG. 2B is a program flowchart depicting one embodiment of a sequence of operations to prepare an authenticatable consumable article.

FIG. 3A is a top right perspective view of a consumable article to be authenticated and a host device in accordance with one embodiment.

FIG. 3B is a top right perspective view of a consumable article for authentication and a host device for authenticating the invention in accordance with one embodiment.

FIG. 4 is a system flow chart illustrating a sequence of operations and flow of data in one embodiment of a method for authenticating a consumable.

FIG. 5 is a cutaway top left perspective view of a consumable article loaded into a host device illustrating the placement of authenticating components in accordance with one embodiment.

FIG. 6 is a cutaway top right perspective view of a consumable article loaded into a host device illustrating the placement of authenticating components in accordance with one embodiment.

FIG. 7A is a perspective view of a consumable article print cartridge with an authenticator circuit mounted on a side in accordance with one embodiment.

FIG. 7B is an enlarged view of an authenticating component mounted on a consumable article.

FIG. 7C is a side orthogonal view of a consumable article print cartridge with an authenticator circuit mounted on a side in accordance with one embodiment.

FIG. 7D is a top orthogonal view of a consumable article print cartridge with an authenticator circuit mounted on a side in accordance with one embodiment.

FIG. 8 is a block diagram of a consumable article, host device, and authenticating circuitry in accordance with one embodiment.

FIG. 9 is a perspective view illustrating placement of a circuit board in a host device for authenticating a consumable article in accordance with one embodiment.

FIG. 10A is a rear orthogonal view of a first embodiment of a circuit board for mounting on a host device to authenticate a consumable article.

FIG. 10B is a front orthogonal view of a first embodiment of a circuit board for mounting on a host device to authenticate a consumable.

FIG. 11 is a perspective view of a consumable article print cartridge spool with an authenticator circuit mounted on a flange in accordance with one embodiment.

FIG. 12A is side orthogonal view of a consumable article print cartridge spool with an authenticator circuit mounted on a flange in accordance with one embodiment.

FIG. 12B is a first end orthogonal view of a consumable article print cartridge spool with an authenticator circuit mounted on a flange in accordance with one embodiment.

FIG. 12C is a second end orthogonal view of a consumable article print cartridge spool with an authenticator circuit mounted on a flange in accordance with one embodiment.

FIG. 12D is a sectional side orthogonal view of a consumable article print cartridge spool with an authenticator circuit mounted on a flange in accordance with one embodiment.

FIG. 13 is a block diagram of a consumable article, host device, and authenticating circuitry in accordance with an embodiment using a network connection.

DETAILED DESCRIPTION

The present description is directed in particular to elements forming part of, or cooperating more directly with, the apparatus in accordance with the invention. It is to be understood that elements not specifically shown or described can take various forms known to those skilled in the art. In this description the term "consumable" refers to a component designed to be used up and replaced in a device referred to as a host. Examples of consumables and their respective hosts include ink jet reservoirs for use in printers, film for use in cameras, a ribbon for use on a typewriter, and/or a toner cartridge for use in a copier.

Referring now to FIG. 1A, a host device (100) is configured to receive a consumable article (120). The host device (100) in this specific embodiment may be a plastic card printer for printing bar codes on plastic cards using a thermal transfer process. The consumable article (120) of this embodiment may be a ribbon cartridge containing a ribbon (150) such as, for example, a resin thermal transfer ribbon or dye sublimation ribbon. A plastic card printer host device (100) can include other conventional components (not show) such as, a print head, magnetic encoder station, power switch, control panel, card feeder, card output hopper, and other components. An openable printer cover (162) conceals the internal mechanism of the ribbon cartridge consumable article (120) and helps limit entry of contaminants, such as dust and particulate matter. A cover release button (160) is shown on one side of the plastic card printer host device (100) in this embodiment. A second cover release button (not shown) may be located on the opposite side. A left interior wall (167L) and a right interior wall (167R) define a slot (165) in the plastic card printer host device (100) for receiving the ribbon cartridge consumable article (120) in this embodiment. The ribbon cartridge consumable article (120) may be loaded into the plastic card printer host device by first pressing the cover release button (160) on a side of the plastic card printer host device (100) to open the printer cover (162) then inserting the ribbon cartridge consumable article (120) vertically into the slot (165) and pressing the ribbon cartridge consumable article (120) into place.

Tactile or audible feedback can indicate that the ribbon cartridge consumable article (120) has been properly seated.

Still referring to the embodiment shown in FIG. 1A, the ribbon cartridge consumable article (120) may include a source spool (140) and a take-up spool (145). Before the ribbon cartridge consumable article (120) is used, the ribbon (150) is disposed in a roll wound about the source spool (140). As the ribbon (150) is used and the ribbon cartridge consumable article (120) is consumed, the ribbon (150) wraps around the take-up spool (145). The source spool (140) and the take-up spool (145) are spaced apart in a fixed relationship in the pictured embodiment by a left brace member (147L) and a right brace member (147R). The source spool (140), the take-up spool (145), the left brace member (147L), and the right brace member (147R) together comprise four sides defining a rectangular shaped space through which the ribbon (150) passes. In the embodiment depicted in FIG. 1A, a radio frequency identification (RFID) transponder (130) is provided on the left brace member (147L) of the ribbon cartridge (120). Although in the pictured embodiment the RFID transponder (130) is disposed on the left brace member (147L), in practice it can also be placed at any suitable location, such as on the right brace member (147R). Of course, the transponder need not be limited to radio frequency signals, and may utilize any form of suitable electromagnetic radiation, such as visible, ultraviolet and infra-red light, as is known in the art.

In accord with the illustrated embodiment of FIG. 1A, the RFID transponder (130) may contain a unique, factory-programmed serial number *n*. Certain commercially available RFID transponders each contain a unique 32 to 64-bit transponder serial identification number, *n*, used in the "anti-collision" protocol. This protocol enables separation and unique identification of several transponders simultaneously appearing in the field of the RFID reader, which may be cause by multiple host devices being located in relatively close proximity.

An authentication number, *x*, is calculated using an encryption function, *F*, selected by and confidential to the manufacturer of the ribbon cartridge consumable article (120). The authentication number is permanently stored on the RFID transponder (130). The encryption function *F* is made available to the printer host device (100) during operation thereof. For example, in one embodiment shown in FIG. 8, the confidential encryption function *F* can be programmed into the printer host device (100) before during manufacture. In another embodiment, the confidential encryption function *F* is made available to the printer host device (100) over a network. When the ribbon cartridge consumable article (120) is loaded into the printer host device (100), the printer's internal RFID transceiver (not shown in FIG. 1A) reads the values of the serial number, *n*, and the authentication number, *x*, from the RFID transponder (130) attached to or on the ribbon cartridge consumable article (120). It then determines whether the authentication number *x* matches the serial number *n* as transformed by the confidential encryption function *F*. If the values agree, then the ribbon cartridge consumable article (120) is deemed to be an authentic media product that is useable on that printer.

Every printer (100) from a given manufacturer may be programmed with the same encryption algorithm at the factory. When the ribbon cartridge consumable article (120) is produced, the same encryption algorithm used to generate the authentication number is provided in the printer. Once the ribbon cartridge consumable article (120) is installed, the transponder's unique serial number, *n*, is read. In a preferred embodiment, transponder's unique serial number, *n*, is already locked into the RFID transponder (130) memory by the manufacturer.

The manufacturer of the ribbon cartridge consumable article (120) also knows the type of media to be made, *y*. In another embodiment, the values of both *n* and also *y* are combined to be used in the encryption algorithm to calculate the authentication code *x*. The manufacturer of the ribbon cartridge consumable article (120) then programs and locks the values *x* and *y* into the transponder (130) memory. The transponder (130) is permanently mounted on to the ribbon cartridge consumable article (120). An effectively unlimited number of unique media rolls or cassettes can be produced in this manner, each containing a uniquely programmed and locked value of serial number *n*, media type number *y*, and authentication number *x*.

Although the serial number *n*, media type number *y*, and the authentication number *x* are freely readable, the confidential encryption function, *F*, are preferably selected from a known class of functions having no obvious inverse. Accordingly, such functions are difficult to decode, thus providing secure authentication. A ribbon cartridge consumable article (120) counterfeiter would have to reconstruct the algorithm *F* available to the printer (100) in order to make a counterfeit ribbon cartridge consumable article (120) work on a printer (100) according to the embodiment depicted in FIG. 1.

If a value of *x* is calculated as some complicated function of the unique and non-copyable transponder serial number *n*, then the values of *n* and *x* can both be stored on the RFID transponder (130), where both numbers are unencrypted and readable by anyone. Optionally, if a media type number, *y*, is also used in the transformation, it can also be stored on the RFID transponder. When the ribbon cartridge consumable article (120) is installed on the printer (100), the printer can read both *x* and *n* (and, optionally, *y*) from the transponder and validate that the read value of *x* is correct for the read value of *n* (and optionally, *y*), thus validating the ribbon cartridge consumable article (120) for the corresponding printer (100).

Judicious selection of an algorithm for *F* from among known strong encryption algorithms can make the breaking of this security system very difficult and, in practice, prohibitively expensive. The authentication code *x* can be calculated using cryptographic methods by applying some function to encrypt *n*. The only information available to the counterfeiter is that a given ribbon's authentication code *x* is correct for a given serial number *n*. More particularly, the counterfeiter will not know or be able to learn how the value of *x* was obtained for a given *n*. Nor can the counterfeiter randomly try all possible values of *n*, because the associated values of *x* will not be known unless the counterfeiter has obtained a valid media roll having both that *n* and the correct authentication code *x*. Thus, the counterfeiter has only limited samples of *n*, *x* to test.

The same is true for embodiments in which *x* is calculated as a function of both the serial number *n* and the media type number *y*. The authentication code *x* can be calculated using cryptographic methods by applying some function to encrypt *n* and *y*. Again, the only information available to the counterfeiter is that a given ribbon's authentication code *x* is correct for a given pair *n*, *y*.

As a further defense against the security system being compromised, a plurality of functions defining acceptable relations among the test values can be stored on the host device. The consumable article can then be programmed with a plurality of authentication codes, each of which satisfies a particular authentication functional relationship. If it is learned that any particular authentication function has been compromised, then media can be validated using one of the other authenticating functions and authentication values. The compromised authentication function can be disabled in the host device to prevent authentication of pirated media made using the compromised authentication function. For example, the compromised authentication function can be disabled in response to a flag set in subsequent media or by updates to the host device software or firmware.

As is know in the art, the host device or printer (100) includes suitable memory, such as RAM, ROM, EEPROM and the like, input/output devices, computer or central processor, optional disc storage and associated support devices, all of which are not shown. The computer may be, for example, an IBM compatible computer having, for example, a Pentium® or Intel family microprocessor. Alternatively, the computer may be APPLE® compatible having a Motorola family microprocessor. However, the computer or central processor may be any computer, processor, central processing unit (CPU), microprocessor, RISC (reduced instruction set computer), mainframe computer, work station, single chip computer, distributed processor, server, controller, micro-controller, discrete logic device, remote computer, internet computer or web computer. The memory and/or the disk storage associated with the computer is configured to store program instructions representing the algorithms and processing steps described herein. Such program instructions may be "downloaded" from disk storage or from non-volatile memory, such as ROM, PROM, EPROM, and the like, or may be downloaded from a remote source via a network or other communication link.

Referring now to the embodiment shown in FIG. 1B, there is shown the plastic card printer host device (100) and ribbon cartridge consumable article (120). In FIG. 1B the ribbon cartridge consumable article (120) is shown loaded into the plastic card printer host device (100). The ribbon cartridge consumable article (120) in this particular embodiment may be inserted between left internal wall (167L) and right internal wall (167R). The RFID transponder is shown mounted on left brace member (147L), but could be mounted elsewhere such as the right brace member (147R). With the ribbon cartridge consumable article (120) loaded, the cover (162) can be closed and the plastic card printer host device (100) operated.

For simplicity of description, the execution of the invention next described will employ only the serial number *n* and the authentication number *x*. However, it is also within the scope of the invention to use a media type number *y* in conjunction with the serial number *n* to compute the authentication number *x*. The use of the serial number *n* can differ from the use of the media type number *y* in that the serial number can be permanently fixed in the RFID transponder when it is manufactured and can be unique to each transponder. On the other hand, the media type number *y* can be stored in the RFID transponder at the factory and is the same for each media of a given type. However, the use of the serial number *n* in the authentication or encryption calculations described here is the same as the use of the media type number *y*.

FIG. 2A is a program flow chart that illustrates one embodiment of a sequence of operations for preparing an authenticatable consumable article to use in a host device. First the manufacturer must choose a suitable authenticating function, which choice is represented by the select authentication function F process (202). The function F if is preferably very difficult to identify given only comparatively few values of x and n. After the select authentication function F process (202), the next step is a read RFID transponder serial number n process (204). The manufacturer of the authenticatable consumable article must read the serial number n from the RFID transponder to be installed on the consumable article. The serial number n is factory installed, and is unique to each transponder. Next, the manufacturer may perform a calculate authentication number $x = F(n)$ process (208). The domain of the function F is not limited to the set of values of n, and in particular F can be a multivariable function as discussed is greater detail below. Having calculated authentication number x with the calculate authentication number $x = F(n)$ process (208), next the authentication number x is placed in the public data area of the transponder with the store authentication number x on RFID transponder process (210).

An alternative embodiment of a sequence of operations for preparing an authenticatable consumable article to use in a host device is illustrated in FIG. 2B. In this embodiment, the manufacturer first selects an authentication function with a select authentication function $F_{M,Q}$ process (202'). The authentication function $F_{M,Q}$ of the process of this alternative embodiment is preferably a classic one-way function used in cryptography, which may be based on the modulo operation and Galois Field arithmetic. Galois Field arithmetic, particularly with the one-way function $([M^G \bmod Q]$, is widely used in public key cryptography. As one example, Diffie-Hellman methods employ this approach. The selection of the parameters M and Q uniquely determines the function $F_{M,Q}(G) = M^G \bmod Q$. As an example, the "modulus" notation may be referred to in an English language sentence in the following way, as is known in the art:

> The value of the function of G is equal to the value of M raised to the power of the value of G "modulo" the value of Q.

The parameters M and Q are two prime values, which are related by M being the primitive element of a prime Galois Field $GF(Q)$ of order Q. After settling on an encryption function in the select authentication function $F_{M,Q}$ process (202'), the next step is the read RFID transponder serial number n process (204). The next step in the embodiment of FIG. 2B, is an identify consumable article type y process (206). The number y is a part number selected by the manufacturer to identify a particular type of media to which the manufacturer will affix this particular RFID transponder. The next step is the select preparatory function $G(n,y)$ process (208). The range of the function $G(n,y)$ becomes the domain of the function $F_{M,Q}(G)$, such that the input values n, y are mapped by the composite function $F \circ G$ to the authentication number x. The function $G(n,y)$ is preferably unique and preferably secret to the manufacture of the authenticatable consumable article. The preparatory function $G(n,y)$ can preferably map each pair n, y to a unique result, although such a one-to-one mapping is not a requirement of the invention. The preparatory function $G(n,y)$ should preferably avoid certain degenerative, pathological values of G. Specifically, the function should preferably avoid resulting in values in the ranges:

$G \leq 0$,

$G = 1$,

$G = \frac{Q-1}{2}$, and

$G = (Q-1)$.

As is known from Galois Field number theory, functions G that produce these values can compromise the security of the encryption function $F_{M,Q}$. An appropriate preparatory function $G(n,y)$ having been selected, the next step in the sequence of operations shown in the particular embodiment illustrated in FIG. 2B is a calculate authentication number $x = F_{M,Q}(G(n,y)))$ process (208). After being calculated, the authentication number x is stored in the public data area on the RFID transponder of one embodiment in the store authentication number x on RFID transponder process (210). Additionally, the number y identifying the media type is stored on the transponder in a store consumable article type number y on RFID transponder process (212), after which the sequence of operations depicted in the embodiment of FIG. 2 for making the consumable media authenticatable is complete.

FIGS. 3A and 3B illustrate another embodiment unloading and loading a consumable article (120A, 120B) out of and into a host device (100) in which the consumable article (120A, 120B) is a ribbon cartridge and the host device (100) is plastic card printer. To unload a ribbon cartridge consumable article (120A, 120B) from a plastic card printer host device (100) after the consumable article has been used, the lid (162) is opened then the ribbon cartridge consumable article in the host device (120B) is lifted out

(310), removing the ribbon cartridge consumable article (120A). To load the ribbon cartridge consumable article (120A), it is inserted vertically (320) and pressed into place (120B).

FIG. 4 is a system flowchart that generally depicts the flow of operations and data flow of a system for one specific embodiment for checking the authenticity of a consumable article loaded in a host device. When a consumable article media is installed on a printer host device, the host device first senses the newly loaded consumable article in a detect consumable article process (410). The consumable article can be detected by a mechanical sensor, by recognizing the proximity of an RFID transponder, or by any other suitable sensor means for such detection. After detection of the new consumable article, the printer's internal RFID transceiver reads from transponder on the installed media the values of the serial number *n*, authentication number *x*, and consumable type *y*.

This is shown in the embodiment illustrated in FIG. 4 as three successive processes, a read serial number *n* process (415), a read consumable type number *y* process (420), and a read authentication number *x* process (425). The order of these operations is not important and can be performed in a different sequence in other embodiments without departing from the scope of the invention. After reading the consumable type number *y*, in the illustrated embodiment of FIG. 4, the validity of the consumable for the particular host is tested in a check consumable type validity process (430). In this embodiment valid types of media *y* for the particular host device are known. If the consumable is of a type invalid for the particular host, the host will report the status of an incompatible cartridge using a report status process (480) and terminate. If the media type is incompatible with the particular host, it is unnecessary to check authenticity of the media.

Referring still to the embodiment of FIG. 4, authentication function data (490) is available for use in checking the authenticity of the consumable media. The host device may be programmed before it is sold with the same authentication function later used to make consumable articles for use in the host device. The sequence of steps defining the authentication function can be stored in the host device as authentication function data (490). If the consumable is of a type *y* valid for the particular host, the authentication number *x* is checked using the authentication function data (490) in a check authentication number process (440). The check authentication number process (440) executes the algorithm defining the authenticating relationship using *n* and *y* as input and compares its internally calculated value of $x = F_{M,Q}(G(n,y))$ with the value of *x* read from the transponder. If they agree, then this is an authenticated media product of type *y* that is useable on that printer. If a roll of media is detected with an improper authentication code *x*, then all validity flags and remaining media counters are reset to zero and locked by a reset flags process (475). This counterfeit media is both detected by the printer, and made unusable for any future application once detected by setting its status as "fully used."

A used consumables list data (470) is made available to the host device in this embodiment to confirm that a previously used up cartridge is not being inserted. After the consumable is validated, it is used in the host in a use consumable process (460) as, for example, by using a ribbon cartridge to print product. In one embodiment, when it is determined that the consumable article has been completely expended by the use consumable process (460), an identifier of the consumable article (such as the unique serial number *n*) will be stored in a used consumable list data (470) indicating that the particular consumable article is completely used. In another embodiment, the used consumable list data (470) can include an identification of all consumable articles loaded into the host device and the percentage of life remaining in each consumable article. The used consumable list data (470) can inexpensively store information regarding a large number of previously used consumables such as, for example, a list of the last 512 print cartridges used in a plastic card printer. If a ribbon cassette or ribbon roll reappears with a higher value of remaining panel count than stored in the plastic card printer memory, the plastic card printer treats the reloaded ribbon cassette or ribbon roll as if it had an invalid authentication, and not only can refuse to use that media, but also can lock its transponder into "fully used" status.

Referring next to the embodiment of FIGS. 5 and 6, there is shown in FIG. 5 a top left perspective cut-away view of an embodiment of a host device containing an authenticatable consumable. FIG. 6 shows a top right perspective cut-away view of an embodiment of a host device containing an authenticatable consumable. The consumable article (120) is shown loaded in the host device (100). A radio frequency identification ("RFID") transponder (130) is shown mounted on the consumable article (120). An antenna (510) in the host device (100) enables it to read information stored in the RFID transponder (130) on the consumable article (100).

Referring next to FIG. 7A-7D there are shown several views illustrating a consumable article. A ribbon cartridge is shown in perspective view in FIG. 7A. The ribbon cartridge consumable article (700) has a source spool (710) on one end, a take up spool (720) on another end, the source spool (710) and the take up spool (720) being connected by a left brace member (730L) and a right brace member (730R). A communications component (740) is shown, which may be a radio frequency identification (RFID) transponder. A print ribbon (750) passes from one spool (710) to the other spool (720) between the brace members (730L, 730R).

FIG. 7B is an expanded view of the communications component (740) RFID transponder label and mounting of an embodiment. The transponder can be located on either the inside or the outside of the left brace member (730L) or the right brace member (730R). A label can also be placed on the brace member describing the RFID transponder.

FIG. 7C is a side orthogonal view of a consumable article (700) according to one specific embodiment. The ribbon cartridge consumable article (700) has a source spool (710) on one end, a take up spool (720) on another end, the source spool (710) and the take up spool (720) being connected by a brace member (730). Mounted on the brace member (730) is a communications component (740), which may be an RFID transponder.

FIG. 7D is a top orthogonal view of a consumable article (700) according to one specific embodiment of the invention. The ribbon cartridge consumable article (700) has a source spool (710) on one end, a take up spool (720) on another end, the source spool (710) and the take up spool (720) being connected by a left brace member (730L) and a right brace member (730R). A communications component (740), which may be an RFID transponder, is mounted on either the left brace member (730L) or the right brace member (730R).

Referring now to FIG. 8, a schematic diagram of a consumable article authentication system for authenticating a consumable article in a host device is shown. A consumable article (800) may include, for example, a print ribbon cartridge having a source spool (805), a take-up spool (810), and a brace member (815). The consumable article (800) may include a communications component (820, 835) for transmitting information to a host device (850). The communications component (820, 835), may in one embodiment, be low-cost RFID transponders, having two specific properties. First, the low-cost type of RFID transponders may preferably include a factory programmed unique serial number *n* (830), which cannot be changed by a user or duplicated by copying a public data area (825) of the transponder into another similar type transponder. Thus each transponder is uniquely numbered, which is a requirement for most types of

RFID transponders that have an "anti-collision" protocol enabling multiple transponders to be differentiated when all are seen in the RFID reader antenna field.

Second, the low-cost RFID transponders preferable has the ability to one-time write (or write and lock) data values, x and y, into a public data area (825) of the transponder. The value y in this particular embodiment is the media type information, since not all media types work on all printer types. The non-zero data value x for this illustrative mode will be a complicated function of y and the unique identification number n of that transponder. The value x in this depicted example will be factory programmed into the transponder at the time the media is made, or at least before it leaves the manufacturer's facility.

Both the Philips I*Code and equivalents and any International Standards Organization ("ISO") 15693 standard compliant 13.56 MHz RFID transponders have a factory-programmed, non-copyable 48-bit serial number with the ability to permanently store a corresponding authentication code (derived from the serial number) in the chip. Section 4.1 of ISO 15693 specifies that each compliant transponder shall be identified by a 64-bit Unique Identifier (UID), which shall be set permanently by the IC manufacturer, and shall be structured as follows:

MSB

LSB

64 57	*56 49*	*48* *1*
'E0' hex	*IC mfr code*	*IC manufacturer serial number*

The most significant byte shall be 'E0' hex, followed by an 8-bit IC manufacturer code, which is assigned per ISO 7816-6/AM1. The 48-bit serial number shall be assigned by the identified IC manufacturer. It is expected that various manufacturers will produce compliant ISO 15693 transponders with factory programmed serial numbers and unique manufacturers' IDs registered under ISO 7816. The manufacturer's unique 8-bit ID, or a list of qualified manufacturers' IDs, can be included as part of the authentication process.

Referring still to the specific embodiment of FIG. 8, a host device (850) includes a communication component (855, 860) for reading the values of n, x, and y stored on the consumable article. A processor (865) can receive the information stored on the consumable article and can use an authentication function (870) $F(M,Q,x,y)$ available to the processor to confirm that an authenticating relationship exists between the authentication code *x* and the serial number *n* and the media type code *y*. . The processor (865) is preferably a secure microprocessor. The printer's media authentication program is hidden from potential piracy by being stored in the secure microprocessor. The authentication program cannot be read out from the printer nor can the program be observed during execution. This helps to prevent a potential pirate from determining or reconstructing the authentication algorithm which calculates *x* for *n* and *y*.

The consumable article preferably includes flags (827) to indicate the number of units of media such as panels of ribbon used on the consumable article. Each ribbon roll core or cassette can only be used once. Other memory elements in the transponder keep track of media usage, and remaining media count. Flags in the transponder memory are reset and locked as each unit portion (typically 10-15%) of that media is used. Since only a maximum of 15% of additional media can be reloaded on the core or cassette, this makes reuse of partially used cores or cassettes economically unattractive. Of course, the flags may be used to indicate any degree of usage.

Referring still to the embodiment illustrated in FIG. 8, there is available to the processor (865) a list of consumables used (880). A "cassettes used" list is kept with in each printer. The last 512 cassette serial numbers *n* and their remaining panel count can be stored in each printer. Should a cassette reappear with a higher value of remaining panel count than stored in the printer memory, the printer can treat the reloaded cassette or ribbon roll as if it had an invalid authentication, and not only refuses to use that media but may lock its transponder into "fully used" status, thus preventing "refilling" of the used media.

Referring next to FIG. 9, there is shown a specific embodiment of a communications component mounted on a host device for reading a communications component on a consumable article. A host device frame (910) is shown. The particular host device frame (910) here depicted is a plastic card printer frame with the exterior plastic housing removed. A circuit board (920) is mounted on the particular host device frame (910). The circuit board (920) includes an antenna (930) for reading a radio frequency identification transponder (not shown). The antenna (930) on the circuit board (920) is a transceiver for reading the transponder (not shown) on a consumable article to be loaded in the host device frame (910). This transceiver is only one embodiment of a communications component of a mode of reading information stored on a consumable article. Other examples of communications components include electrical contacts for completing a circuit, infrared or other light sensors for communicating with an LED or the like, a mechanical switch set by, for example, electromechanical means, or any suitable means for communicating such a signal.

One embodiment of a circuit board suitable for practicing one mode of the invention is shown in FIG. 10A and FIG. 10B. FIG. 10A is the obverse of the circuit board and FIG. 10B is the reverse. A receptacle (1015) is provided on the circuit board in this particular embodiment for including a microprocessor. As described with respect to Fig. 8, The printer's media authentication program is preferably hidden from potentially piracy by being stored in a secure microprocessor.

Referring next to FIG. 11, an alternative embodiment of a communications component for mounting on a consumable article is shown. A spool (1310) is provided for use in a consumable article. In one embodiment the consumable article can be, for example, a ribbon cartridge for use in a host device. In another embodiment the consumable article can be, for example, a roll of film for use in a camera. The ribbon or media is wound about the spool (1310). A flange (1320) is associated with the spool (1310). The flange (1320) can be located on one end of the spool (1310) or at any convenient location associated with the spool (1310). In the illustrated embodiment, conductive strips (1330) disposed on the flange in concentric rings serve as a communications component to transmit information stored on the consumable article to a host device.

Referring next to FIG. 12A-12D, there are shown several views of a part for use in a consumable article. FIG. 12A is a side orthogonal view of a winding spool (1405). A winding drum (1410) is provided about which media can be wound, such as ribbon in a print cartridge for use in a printer or film in a roll of film for use in a camera. A flange (1415) is associated with the winding drum and can, for example, be attached to one end of the winding drum. Other configurations are possible and are considered to be equivalent. A communications component can be mounted on the flange for communicating with a host device such as a printer or camera.

FIG 12B is an end orthogonal view from the end opposite the flange (1415) on the winding drum (1410). In the particular embodiment shown, the winding drum (1410) is hollow, having an interior surface (1420) defining a cavity. FIG. 12C is an end orthogonal view from the end on which the flange (1415) is mounted. Again visible is the interior surface (1420) defining the hollow cylindrical cavity found in this particular embodiment.

Referring now to FIG. 12D, there is shown a sectional view along cut line A-A of the view shown in FIG. 12A. The spindle (1405) has a winding drum (1410) with an outer surface (1425) about which media such as a ribbon for a printer or film for a camera can be wrapped. An interior surface (1420) in this embodiment defines a cavity in the hollow interior. A flange (1415) on one end can be used to mount a communications component, such as an RFID transponder. In an alternate embodiment, a first communications component (1430), such as an RFID transponder, may be mounted on the interior surface (1420), which communicates with the host device by means of a second communication component (not shown) disposed axially within the hollow cavity defined by the interior wall of the spool.

Referring now to FIG. 13, there is disclosed a schematic diagram of a consumable article authentication system for authenticating a consumable article in a host device. A consumable article (1500) may include, for example, a print ribbon cartridge having a source spool (1505), a take-up spool (1510), and a brace member (1515). The consumable article (1500) may include a communications component (1520, 1535) for transmitting information to a host device (1550). In one embodiment, the communications component (1520, 1535), may be a low-cost RFID transponder having two specific properties. First, the low-cost RFID transponders can preferably include a factory programmed unique serial number *n* (1530), which cannot be changed by a user, or duplicated by copying a public data area (1525) of the transponder into another similar type transponder. Thus each transponder is uniquely numbered, which is a requirement for most types of RFID transponders that have an "anti-collision" protocol enabling multiple transponders to be differentiated when all are seen in the RFID reader antenna field.

Second, the low-cost type of RFID transponders can preferably have the ability to one-time write (or write and lock) data values, *x* and *y*, into a public data area (1525) of the transponder. The value *y* in this particular embodiment is the media type information, since not all medias work on all printer types. The non-zero data value, *x*, for this illustrative mode will be a complicated function of *y* and the unique identification number *n* of that transponder. The value *x* in this depicted example can be factory programmed into the transponder at the time the media is made, or at least before it leaves the manufacturer's warehouse.

Also shown is a host device (1550), which includes a communication component (1555, 1560) for reading the values of *n*, *x*, and *y* stored on the consumable article. A processor (1565) can receive the information stored on the consumable article and can use an authentication function (1570) $F(M,Q,x,y)$ available to the processor to confirm that an authenticating relationship exists between the authentication code x and the serial number n and the media type code y. The processor (1565) can be remote from the host device and may communicate with the host device through a communications channel (1590), such as a network or a telecommunications link.

The consumable article preferably includes flags (1527) to indicate the number of units of media, such as panels of ribbon, used on the consumable article. Each ribbon roll core or cassette can only be used once. Other memory elements in the transponder keep track of media usage, and remaining media count. Flags in the transponder memory can be reset and locked as each portion (typically 10-15%) of that media is used. Because only a maximum of 15% of additional media can be reloaded on the core or cassette, this makes reuse of partially used cores or cassettes economically unattractive.

Referring still FIG. 13, there is available to the processor (1565) a list of consumables used (1580). A "cassettes used" list is kept in each printer. The last 512 cassette serial numbers n and their remaining panel count are stored in each printer. Should a cassette reappear with a higher value of remaining panel count than stored in the printer memory, the printer treats the reloaded cassette or ribbon roll as if it had an invalid authentication, and not only refuses to use that media but locks its transponder into "fully used" status.

Implementation of the above described method and apparatus includes repeated operations of the form M^N, where M and N are both large prime numbers. When M and N are both large prime numbers, then M^N can be theoretically become hundreds of digits (or bits). To better implement the above described authentication algorithm, a method has been derived that allows both M^N to be quickly evaluated in a small microprocessor and restrict the number of bits to twice the length of Q.

As an example, assume that $M << Q$ and Q is 64 bits, so that a 64-bit times 64-bit multiply (128-bit result) is all that is required. This example is offered by way of illustration, and other embodiments are possible.

Let N be defined as a 64-bit binary number, which is some function of n and y:

$$N(n,y) = c_o 2^0 + c_1 2^1 + \ldots + c_{63} 2^{63} = \sum_{i=0}^{63} c_i 2^i \qquad \text{Equation 1}$$

In this equation, each c_i represents successive binary digits. Substituting the above into M^N yields:

$$\begin{aligned} M^N &= M^{c_0 2^0 + c_1 2^1 + \ldots + c_{63} 2^{63}} = M^{\sum_{i=0}^{63} c_i 2^i} \\ M^N &= \prod_{i=0}^{63} M^{c_i 2^i} \end{aligned} \tag{Equation 2}$$

Using this transformation of M^N, the equation $M^N \bmod Q$ can be evaluated using the lemma:

$$(a \times b) \bmod c = [(a \bmod c) \times (b \bmod c)] \bmod c \tag{Equation 3}$$

Applying this lemma yields:

$$M^N \bmod Q = \left(\prod_{i=0}^{63} \left(M^{c_i 2^i} \right) \bmod Q \right) \bmod Q \tag{Equation 4}$$

Letting

$$T_i = \left(M^{c_i 2^i} \right) \bmod Q \tag{Equation 5}$$

then

$$M^N \bmod Q = \left(\prod_{i=0}^{63} T_i \right) \bmod Q \tag{Equation 6}$$

Each term T_i can now be evaluated using the fact that each c_i is either 0 or 1.

$$\begin{aligned} &\text{if } c_i = 0 \text{ then } T_i = M^{c_i 2^i} \bmod Q = M^0 \bmod Q = 1 \\ &\text{if } c_i = 1 \text{ then } T_i = M^{c_i 2^i} \bmod Q = M^{2^i} \bmod Q \end{aligned} \tag{Equation 7}$$

The up to 64 values of T_i for $c_i = 1$ can be either be previously calculated and stored in a table or can be sequentially evaluated. Using this table or these calculated values for T_i, the value of $M^N \bmod Q$ can be evaluated progressively. Let P_i be the partial product at each stage, i, from 1 to 63. Calculating in a recursive, pair-wise manner:

$$\begin{aligned} P_i &= (T_0 \times T_1) \bmod Q \\ P_2 &= (P_1 \times T_2) \bmod Q \\ &\vdots \\ P_i &= (P_{i-1} \times T_i) \bmod Q \end{aligned} \tag{Equation 8}$$

until

$$M^N \bmod Q = P_{63} = (P_{62} \times T_{63}) \bmod Q \tag{Equation 9}$$

Using the fact that when $c_i = 0$ then $T_i = 1$ cuts the number of 64x64 bit multiplication operations by 50% on the average. In order to implement the security system described herein, however, there remains a need for a fast 64-bit modulo Q operation on a 128-bit number.

For each of the steps above when $c_i = 1$ a reduction of form $(W \bmod Q)$ must be performed. Normally, this is done by an integer long division operation to find the integer remainder. In the case here, where the divisor Q is of order 64 bits and the dividend W is of order 128 bits, a great number of shift and subtract operations must be performed.

To better implement the security system described herein, a method that is approximately 20 times faster than long division has been developed. Assume that Q is chosen to be

$$Q = 2^n - k, \text{ where } k << 2^n \qquad \text{Equation 10}$$

This includes the Mersenne Prime numbers, of form $2^n - 1$. But, if $(W \operatorname{div} Q)$ can be accurately estimated (that is, the integer quotient of the division operation) then the remainder can easily be easily found by:

$$W \bmod Q = W - Q \times (W \operatorname{div} Q) \qquad \text{Equation 11}$$

The integer quotient of the division operation can be estimated as follows. First, write the equivalence

$$W \operatorname{div} Q = \operatorname{int}\left(\frac{W}{2^n - k}\right) \qquad \text{Equation 12}$$

Multiplying both the numerator and denominator of the right side by 2^{-n} yields

$$W \operatorname{div} Q = \operatorname{int} \frac{2^{-n} W}{1 - 2^{-n} k} \qquad \text{Equation 13}$$

Because Q is typically larger (here on the order of $n \sim 63$ bits), then $(2^{-n}\,k) << 1$ and the denominator in Equation 14 can be expanded using the infinite series

$$\frac{1}{1-u} = \sum_{i=0}^{\infty} u^i \qquad \text{Equation 14}$$

Substituting Equation 14 into Equation 13 yields:

$$W \operatorname{div} Q = \operatorname{int}\left(2^{-n} W \sum_{i=0}^{\infty} (2^{-n} k)^i\right) \qquad \text{Equation 15}$$

Evaluating the first few terms of Equation 15 reveals that

$$W \operatorname{div} Q \approx \operatorname{int}\left(2^{-n} W + w^{-2n} k W + 2^{-3n} k^2 W + \ldots\right) \qquad \text{Equation 16}$$

Knowing the maximum values of n, k, and W, one can evaluate the terms of Equation 16 until the first term is found which is sufficiently small (such as less than ½) so that further terms will not affect the integer portion since all subsequent terms will be smaller. These terms that will not affect the value of the integer portion can then be safely ignored in the evaluation of Equation 16.

In practice, W, Q and k can be chosen so that Equation 16 converges after only a few terms. This method of calculating $W \bmod Q$ proves in practice to be many times faster than finding it by long division directly.

As another example of an alternate embodiment, the consumable and the host can communicate by an optical coupling. Other examples include electrical contracts and magnetic read-write heads. This invention is not limited to any of the particular exemplary modes of communication between the consumable and the host enumerated in this description, and the claims below are intended to cover any suitable mode of communication.

Whereas the invention has been described as being preferably applied to a media processing system in the form of a thermal transfer printer, the invention has equal applicability to thermal printers, such as described in US patents 5,266,968 and 5,455,617, photoprocessing apparatus, such as described in US patent 6,106,166, photographic cameras, such as described in US patent 6,173,119, X-ray cameras, such as described in US patent 5,428,659, ink jet printers, laser printers, and the like. Whereas the invention has been depicted as applied to a media processing system wherein the media assembly and media processing system communicate wirelessly, the invention is also readily adapted for use in systems wherein the media assembly and media processing system communicate by a wired connection, as shown in US patents 5,266,968 and 5,455,617.

Specific embodiments of the present method and apparatus have been described for the purpose of illustrating the manner in which the invention may be made and used. It should be understood that implementation of other variations and modifications of the invention and its various aspects will be apparent to those skilled in the art, and that the invention is not limited by the specific embodiments described. It is therefore contemplated to cover by the present invention any and all modifications, variations, or equivalents that fall within the true spirit and scope of the basic underlying principles disclosed and claimed herein.

IN THE CLAIMS

I CLAIM:

1. An authentication method for authenticating an article in a device, the method comprising the steps of:

reading an identification number stored on the article;

reading an authentication number stored on the article;

determining an input number based at least in part on the identification number;

applying an authentication function to the input number to calculate an output number;

determining that the article is authentic only if the authentication number corresponds to the output number; and

permitting use of the article in the device if the article is authentic, and disabling use of the article in the device if the article is not authentic.

2. The authentication method according to claim 1 wherein the authentication function is an encryption transformation of the input number.

3. The authentication method according to claim 1 further comprising the step of reading a media type number stored on the article.

4. The authentication method according to claim 3 further comprising the step of determining the input number based at least in part on the media type number.

5. The authentication method according to claim 2 wherein the step of applying the encryption transformation further comprises the steps of:

providing a first prime number, Q;

providing a second prime number, M;

the second prime number being a primitive element of the prime Galois Field of the first prime number; and calculating the output number according to the formula:

output number = M^N MOD Q, where N is the input number.

6. The authentication method according to claim 5 wherein the second prime number is selected such that the second prime number is greater than 0, the second prime number is not equal to 1, and the second prime number is not equal to one-half of, the first prime number minus 1.

7. The authentication method according to claim 5 wherein determining the output number further comprises the steps of:

a) initializing a partial product by:

setting a multiplier equal to the second prime number;

setting the partial product equal to 1 if the least significant bit of the input number is equal to 0;

setting the partial product equal to the multiplier modulo the first prime number if the least significant bit of the input number is equal to 1;

b) from the least significant bit to the most significant bit of the input number, for each such bit, iteratively evaluating the partial product by:

doubling the multiplier;

resetting the partial product equal to the prior partial product modulo the first prime number if a next unevaluated bit of the input number is equal to 0;

resetting the partial product equal to (a) the prior partial product times the modulo of the multiplier over the second prime number (b) modulo the second prime number, if said next unevaluated bit of the input number is equal to 1; and

c) concluding said iterative evaluation of the partial product after evaluating the partial product for the most significant bit of the input number.

8. The authentication method according to claim 1 further comprising the steps of:

providing a counter on the article, the counter configured to be read by the device;

periodically updating an article usage value in the counter as the article is used to reflect an extent of usage or depletion of the article;

reading the article usage value by the device;

determining that the article is authentic only if the article usage value is greater than a predetermined value; and

permitting use of the article in the device if the article is authentic, and disabling use of the article in the device if the article is not authentic.

9. The authentication method according to claim 8 further comprising the steps of:

providing a table accessible by the device, the table containing the identification numbers corresponding to a plurality of the articles used in the device;

each identification number having an associated entry in the table corresponding to a last read article usage value of each article used in the device;

determining that the article installed in the device is authentic only if its article usage value is less than the last read article usage value for the corresponding identification number in the table; and

permitting use of the article in the device if the article is authentic, and disabling use of the article in the device if the article is not authentic

10. The authentication method according to claim 1 further comprising the step of mounting an RFID transponder on the article wherein the identification number and the authentication number are stored in the RFID transponder.

11. The authentication method according to claim 1 further comprising the step of mounting an RFID transceiver on the device.

12. A device configured to authenticate an article installable in the device, the device comprising:

a reader adapted to read an identification number stored on the article, the identification number corresponding to an identification of the article;

the reader further adapted to read an authentication number stored on the article;

a memory of the device containing a computer program configured to transform the identification number into an output number and compare the output number to the authentication number; and

the article being authenticated only if the output number is equal to the authentication number, wherein use of the article in the device is permitted if the article is authentic, and use of the article in the device is not permitted if the article is not authentic.

13. The device according to claim 12 wherein the reader is a transceiver mounted on the device.

14. The device according to claim 12 wherein the computer program that transforms the identification number into an output number comprises:

a preparatory computer program in a memory of the device configured to transform the identification number into an intermediate number;

an encryption computer program in a memory of the device configured to encrypt the intermediate number to provide the output number; and

wherein the output number is compared to the authentication number to determine the authenticity of the article in the device.

15. The device according to claim 14 in which the preparatory computer program performs a one-to-one transform so that the intermediate number is equal to the identification number.

16. The device according to claim 12 wherein the reader is configured to read a media type number stored on the article.

17. The device according to claim 15 wherein the preparatory program uses the media type number as input to calculate the intermediate number.

18. The device according to claim 14 wherein the encryption computer program is contained in a computer readable medium that calculates (a) a second prime number raised to the power of the intermediate value (b) modulo a first prime number.

19. The device according to claim 18 wherein the second prime number is selected such that the second prime number is greater than 0, the second prime number is not equal to 1, and the second prime number is not equal to one-half of, the first prime number minus 1.

20. The device according to claim 18 wherein the encryption computer program contained in a computer readable medium further comprises:

a) a computer program initialization code segment that

(i) sets a multiplier equal to the second prime number;

(ii) sets the partial product equal to 1 if the least significant bit of the intermediate number is equal to 0;

(iii) sets the partial product equal to the multiplier modulo the first prime number if the least significant bit of the intermediate number is equal to 1;

b) a computer program partial product evaluation code segment that evaluates the partial product iteratively from the least significant bit of the intermediate number to the most significant bit of the intermediate number by

(i) doubling the multiplier;

(ii) resetting the partial product equal to the prior partial product modulo the first prime number if a next unevaluated bit of the intermediate number is equal to 0;

(iii) resetting the partial product equal to (a) the prior partial product times the modulo of the multiplier over the second prime number (b) modulo the second prime number, if said next unevaluated bit of the intermediate number is equal to 1;

c) terminates an iterative evaluation of the partial product after evaluating the partial product corresponding to the most significant bit of the intermediate number; and

d) outputs the final partial product as the output number.

21. The device according to claim 20 further comprising a memory for storing a table with an entry for each bit of the intermediate number, the contents of the entry being equal to the multiplier corresponding to that bit, modulo the first prime number.

22. The device according to claim 12 wherein the computer program includes code configured to produce a plurality of output numbers, and wherein the article is authenticated only if one of the plurality of output numbers is equal to the authentication number.

23. The device according to claim 12 further including a counter on the article, the counter configured to be read by the device wherein the reader reads an article usage value in the counter, the article usage value reflecting an extent of usage or depletion of the article.

24. The device according to claim 12 wherein the memory further includes

a table accessible by the device, the table containing the identification numbers corresponding to a plurality of the articles used in the device; and

each identification number having an associated entry in the table corresponding to a last read article usage value of each article used in the device, and wherein the computer program determines that the article installed in the device is authentic only if its article usage value is less than the last read article usage value for the corresponding identification number in the table, and permits use of the article in the device if the article is authentic and disables use of the article in the device if the article is not authentic.

25. A host device configured to authenticate an article, the host device comprising:

means for reading an identification number stored on the article;

means for reading an authentication number stored on the article;

means for determining an input number based at least in part on the identification number;

means for applying an authentication function to the input number to calculate an output number;

means for determining that the article is authentic only if the authentication number corresponds to the output number; and

means for permitting use of the article in the device if the article is authentic, and disabling use of the article in the device if the article is not authentic.

26. An article adapted to be authenticated by a host device, the article comprising a memory system configured to store a first predetermined number and an authentication number, the first predetermined number corresponding to an identification of the article.

27. The article according to claim 26 wherein the authentication number is calculated by applying an authentication algorithm to the first predetermined number.

28 The article according to claim 27 wherein the predetermined number is a unique, factory installed serial number.

29. The article according to claim 26 wherein the authentication number is calculated by:

providing a first prime number, Q;

providing a second prime number, M;

the second prime number being a primitive element of the prime Galois Field of the first prime number; and

calculating the output number according to the formula:

output number = M^N MOD Q, where N is the first predetermined number.

30. The article according to claim 29 wherein the second prime number is selected such that the second prime number is greater than 0, the second prime number is not equal to 1, and the second prime number is not equal to one-half of, the first prime number minus 1.

31. The article according to claim 29 wherein the step of determining the output number further comprises the steps of:

a) initializing a partial product by:

setting a multiplier equal to the second prime number;

setting the partial product equal to 1 if the least significant bit of the first predetermined number is equal to 0;

setting the partial product equal to the multiplier modulo the first prime number if the least significant bit of the predetermined number is equal to 1;

b) evaluating the partial product iteratively from the least significant bit of the first predetermined number to the most significant bit of the first predetermined number by:

doubling the multiplier;

resetting the partial product equal to the prior partial product modulo the first prime number if a next unevaluated bit of the first predetermined number is equal to 0;

resetting the partial product equal to (a) the prior partial product times the modulo of the multiplier over the second prime number (b) modulo the second prime number, if said next unevaluated bit of the first predetermined number is equal to 1; and

c) terminating the iteratively evaluation of the partial product after evaluating the partial product for the most significant bit of the first predetermined number.

32. A computer program product comprising:

a computer readable medium containing computer program code, the computer program code providing a first prime, a second prime number that is a primitive element of the prime Galois Field of the first prime number, and an input value, the computer program code having

a) a computer program code that initializes a partial product by

(i) setting a multiplier equal to the second prime number;

(ii) setting the partial product equal to 1 if the least significant bit of the input number is equal to 0;

(iii) setting the partial product equal to the multiplier modulo the first prime number if the least significant bit of the input number is equal to 1;

b) a computer program code that evaluates the partial product iteratively from the least significant bit of the input number to the most significant bit of the input number by

(i) doubling the multiplier;

(ii) resetting the partial product equal to the prior partial product modulo the first prime number if a next unevaluated bit of the input number equal to 0;

(iii) resetting the partial product equal to (a) the prior partial product times the modulo of the multiplier over the second prime number (b) modulo the second prime number, if said next unevaluated bit of the input number is equal to 1; and wherein

c) a computer program code that terminates an iterative evaluation of the partial product after evaluating the partial product for the most significant bit of the input number.

The computer program product according to claim 0, wherein the computer program code that iteratively evaluates the partial product further includes forming a table with an entry for each bit of the input number, the contents of the entry being equal to the multiplier corresponding to that bit, modulo the first prime number, wherein iterative evaluations of the partial product access the table entries.

33. An apparatus for determining a remainder of an integer division, the apparatus comprising:

a memory;

a dividend storage location in the memory;

an exponent storage location in the memory;

a subtrahend storage location in the memory;

a divisor storage location in the memory, the quantity stored in the divisor storage location being equal to the quantity stored in the subtrahend location subtracted from two raised to the power of the quantity stored in the exponent location;

a summation algorithm stored in the memory, the algorithm summing the terms of a series equal to the quotient of the quantity stored in the dividend storage location divided by the quantity stored in the divisor storage location, the algorithm halting with the first term of the series that is less than one half; and a modulo algorithm stored in the computer memory that computes the remainder by subtracting from the quantity stored in the dividend storage location the quantity stored in the product of the quantity stored in the divisor storage location multiplied by the integer portion of the quantity determined by the summation algorithm.

34. For use with a thermal transfer, thermal or other printer, or photographic or X-ray camera, or other media processing system, a media assembly configured to identify and disable used of counterfeit media, the media assembly comprising an anti-counterfeiting provision having a data store containing encrypted data and reference data uniquely associated with the media assembly; and a processor configured to access the encrypted data and reference data and configured to permit usage of the media if the media is not counterfeit.

35. The apparatus defined by claim 34 wherein the data store also holds reference data.

36. The assembly defined by claim 34 wherein said encrypted data represents a secure transform function of said reference data.

37. The assembly defined by claim 34 wherein said encrypted data is derived by applying an encryption algorithm to the reference data.

38. The assembly defined by claim 34 wherein said encrypted data is derived by employing a one-way function.

39. The assembly defined by claim 34 wherein said data store also contains media type data representing a type or model of the media.

40. The assembly defined by claim 34 wherein said anti-counterfeiting provision includes an RFID transponder.

41. The assembly defined by claim 40 wherein said transponder includes a memory which constitutes said data store.

42. The assembly defined by claim 41 wherein said anti-counterfeiting provision is responsive to electromagnetic signals in the visible, infra-red or ultraviolet spectra.

43. The apparatus defined by claim 34 wherein said data store is a transponder memory.

44. The apparatus defined by claim 34 wherein said anti-counterfeiting provision includes an RFID transponder having a memory constituting said data store.

45. The apparatus defined by claim 34 wherein said media processing system is a thermal transfer printer, and wherein said media is a thermal transfer ribbon.

46. The apparatus defined by claim 34 wherein said media processing system is a thermal transfer printer, and wherein said media is a direct thermal recording media.

47. For use with a thermal transfer, thermal or other printer, or photographic or X-ray camera, or other media processor, a media holder in the form of a spool having a shaft with an axis and an end flange, on which is located an antenna.

48. The apparatus defined by claim 47 wherein said antenna comprises at least one arcuate conductor concentric with said shaft axis.

49. The apparatus defined by claim 47 wherein said antenna comprises a series of coupled concentric circular conductors supported on said end flange of said spool.

50. The apparatus defined by claim 49 wherein said conductors comprise deposited traces.

51. The apparatus defined by claim 47 wherein said antenna is connected to a data memory.

52. The apparatus defined by claim 51 wherein said data memory contains encrypted data.

53. The apparatus defined by claim 47 wherein said antenna comprises part of a wireless transponder.

54. The apparatus defined by claim 53 wherein said transponder is an RFID transponder.

55. The system defined by claim 47 wherein said media processor includes a media usage counter configured to track media usage and store a usage indication on the media assembly.

56. The system defined by claim 55 wherein said usage indication is used to reject a media assembly having a recorded usage great than or equal to a predetermined usage value.

57. The system defined by claim 55 wherein said media processor is a laser printer.

58. A thermal transfer, thermal or other printer, or photographic or X-ray camera, or other media processing system adapted to identify a counterfeit media assembly, said system including a program configured to execute an encryption algorithm employed to validate a media assembly.

59. The system defined by claim 58 wherein said algorithm is executed in a secure microprocessor.

60. The system defined by claim 58 wherein said system includes a media processor, and wherein said program resides on said media processor.

61. The system defined by claim 58 wherein said system includes a media processor and a remote processing station, and wherein said program resides on said remote processing station.

62. The system defined by claim 58 wherein said encryption algorithm operates on data stored on the media assembly.

63. The system defined by claim 62 wherein said data includes reference data and encrypted data derived from said reference data.

64. The system defined by claim 63 wherein said encrypted data is developed employing said encryption algorithm.

65. The system defined by claim 58 wherein said encryption algorithm comprises a one-way function.

66. The system defined by claim 65 wherein said one-way function utilizes modulo arithmetic in a Galois Field.

FIG. 1A

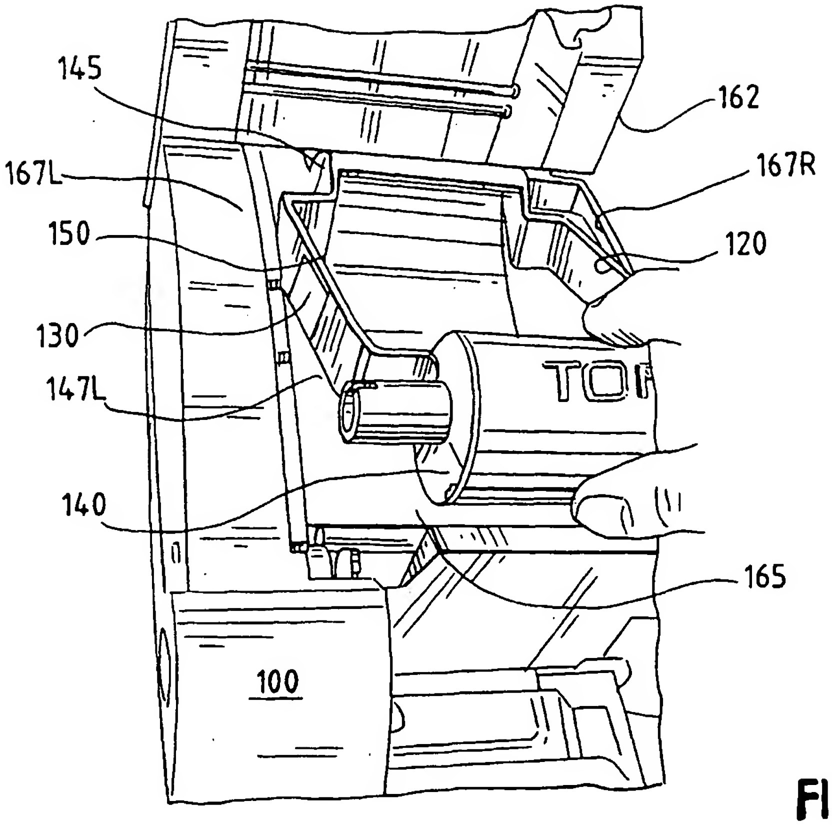

145
162
167L
167R
150
120
130
147L
TOP
140
165
100

FIG. 1B

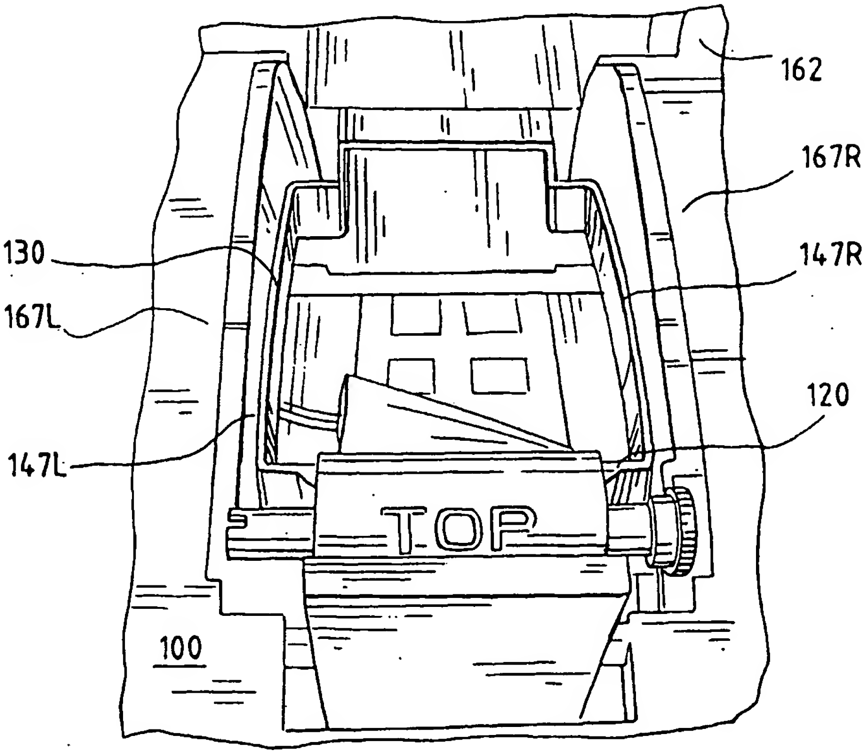

162
167R
130
147R
167L
120
147L
TOP
100

FIG. 2A

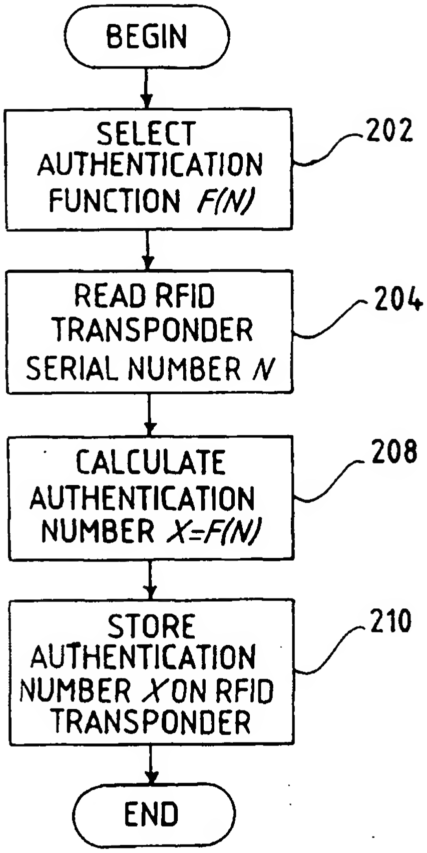

BEGIN
SELECT AUTHENTICATION FUNCTION $F(N)$
202
READ RFID TRANSPONDER SERIAL NUMBER N
204
CALCULATE AUTHENTICATION NUMBER $X=F(N)$
208
STORE AUTHENTICATION NUMBER X ON RFID TRANSPONDER
210
END

FIG. 2B

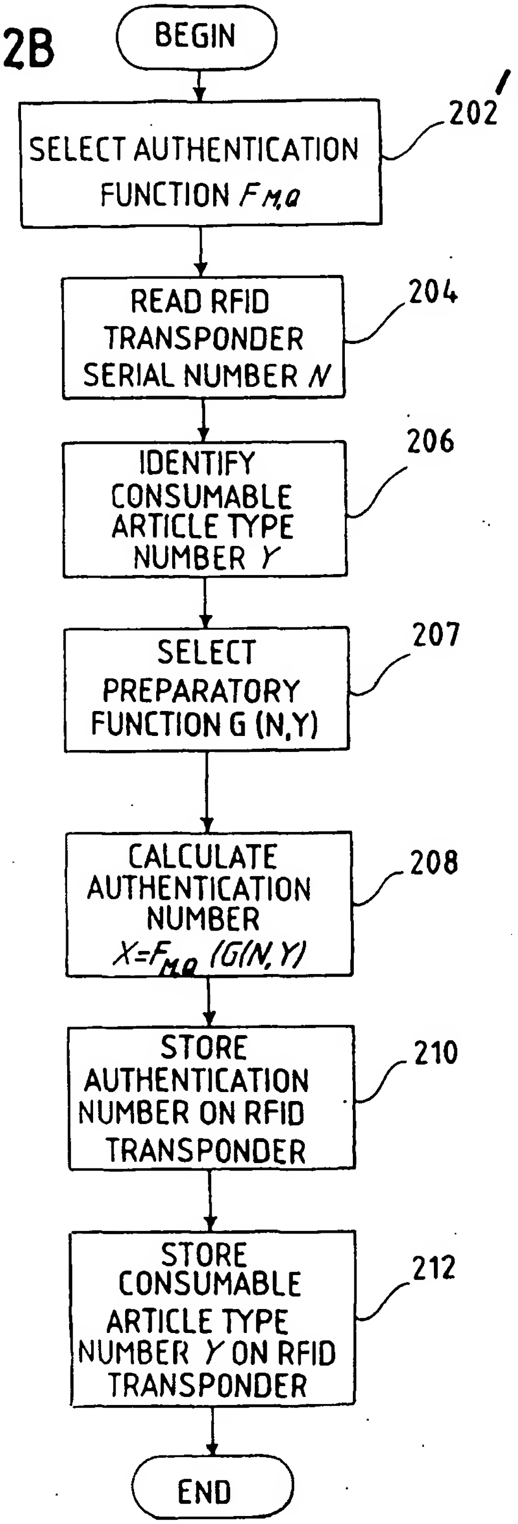

BEGIN
SELECT AUTHENTICATION FUNCTION $F_{M,Q}$
202'
READ RFID TRANSPONDER SERIAL NUMBER N
204
IDENTIFY CONSUMABLE ARTICLE TYPE NUMBER Y
206
SELECT PREPARATORY FUNCTION G (N,Y)
207
CALCULATE AUTHENTICATION NUMBER $X=F_{M,Q}(G(N,Y)$
208
STORE AUTHENTICATION NUMBER ON RFID TRANSPONDER
210
STORE CONSUMABLE ARTICLE TYPE NUMBER Y ON RFID TRANSPONDER
212
END

FIG. 3A

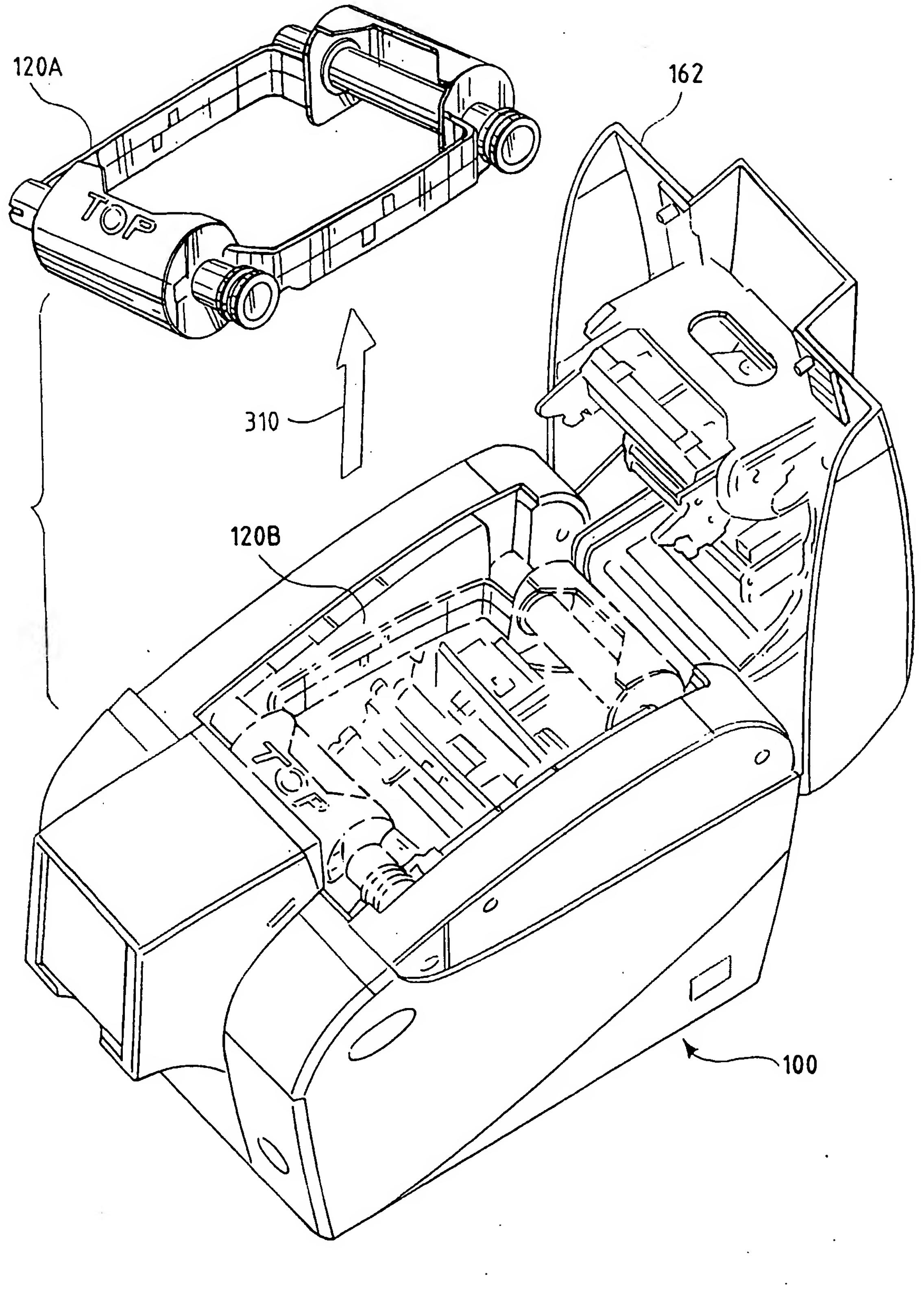


FIG. 3B

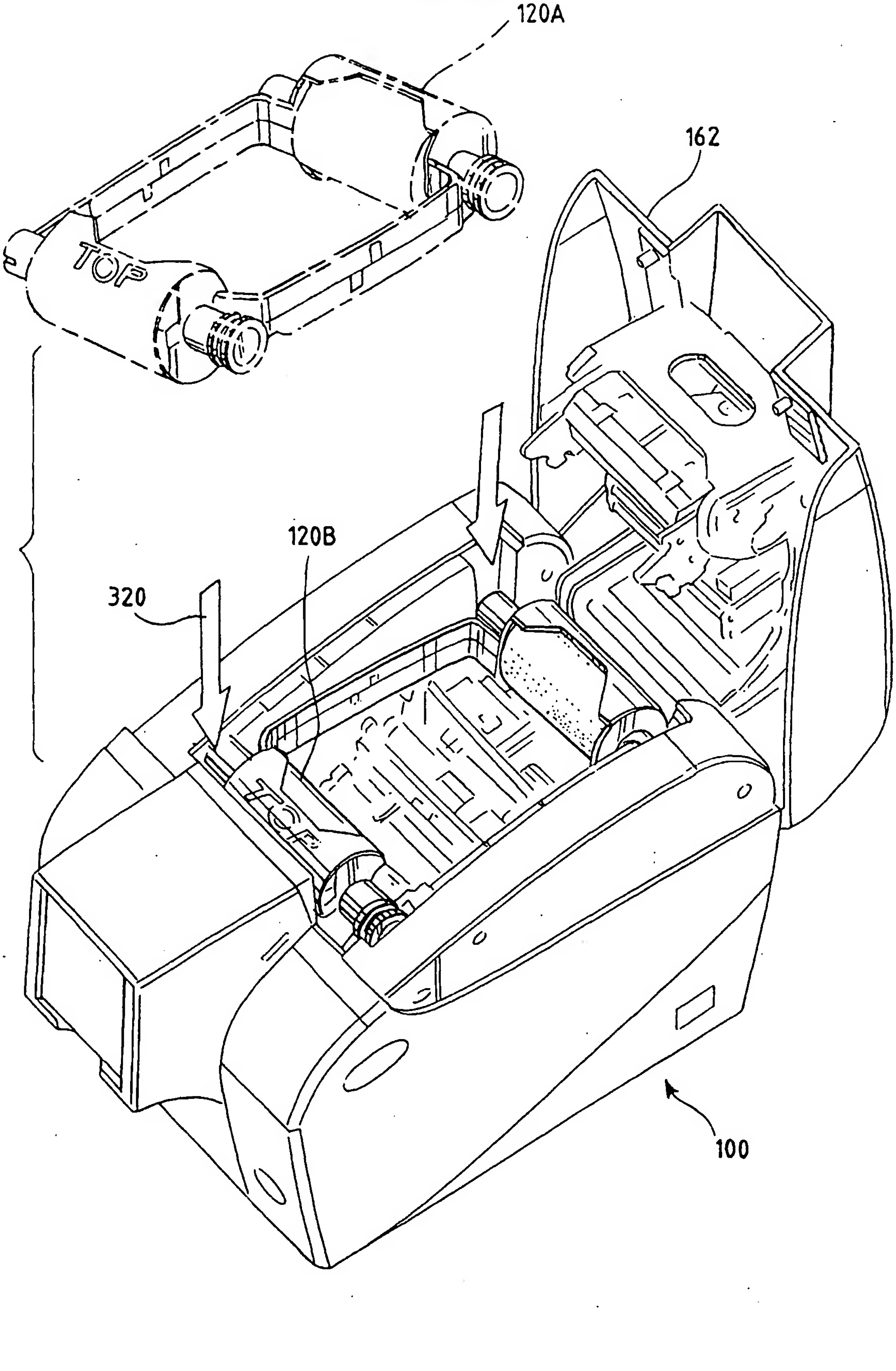


FIG. 4

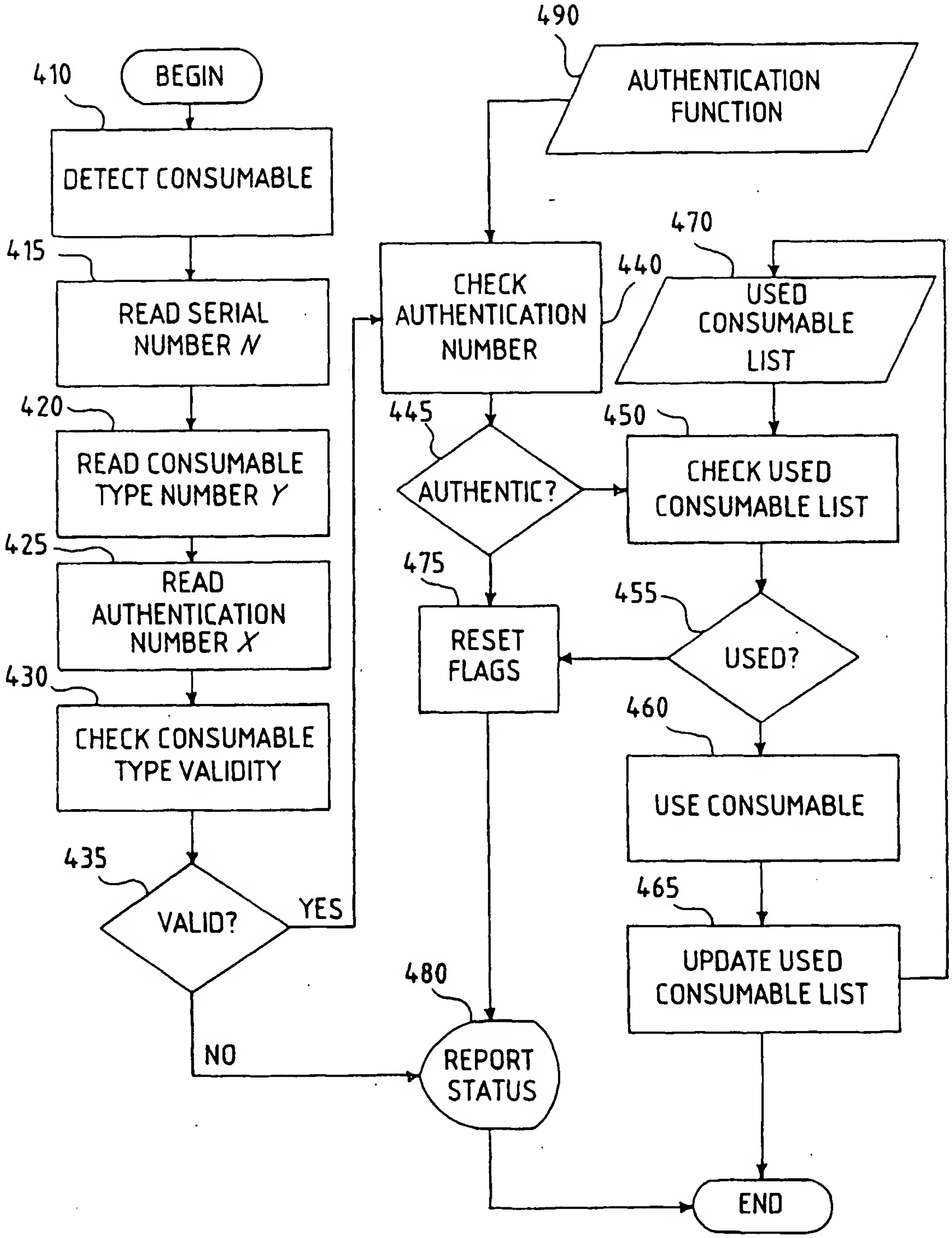

490
AUTHENTICATION FUNCTION
410
BEGIN
DETECT CONSUMABLE
415
READ SERIAL NUMBER N
420
READ CONSUMABLE TYPE NUMBER Y
425
READ AUTHENTICATION NUMBER X
430
CHECK CONSUMABLE TYPE VALIDITY
435
VALID?
YES
NO
CHECK AUTHENTICATION NUMBER
440
470
USED CONSUMABLE LIST
445
AUTHENTIC?
450
CHECK USED CONSUMABLE LIST
475
RESET FLAGS
455
USED?
460
USE CONSUMABLE
465
UPDATE USED CONSUMABLE LIST
480
REPORT STATUS
END

FIG. 5

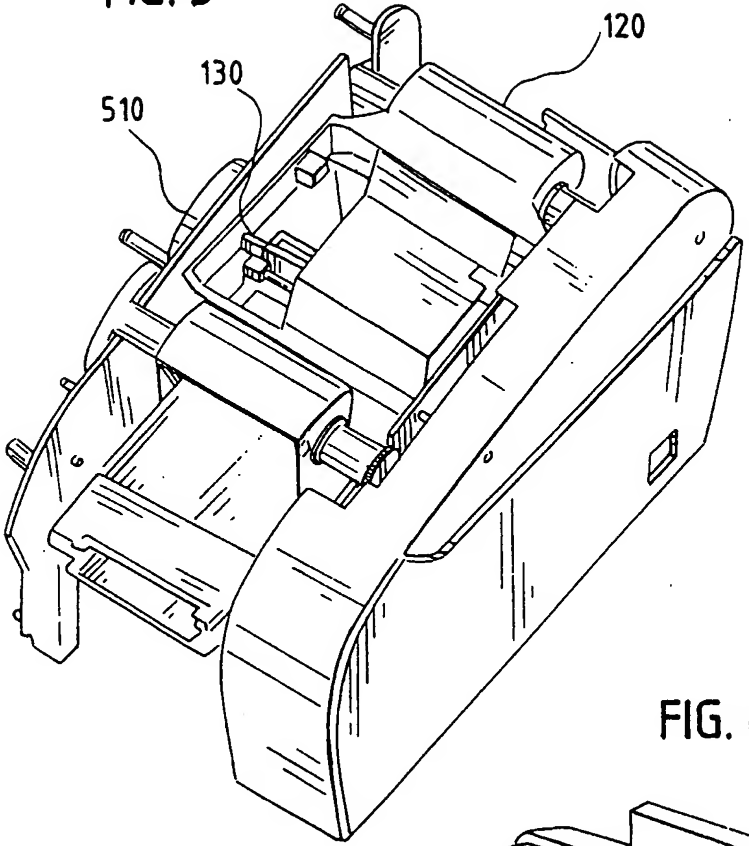


FIG. 6

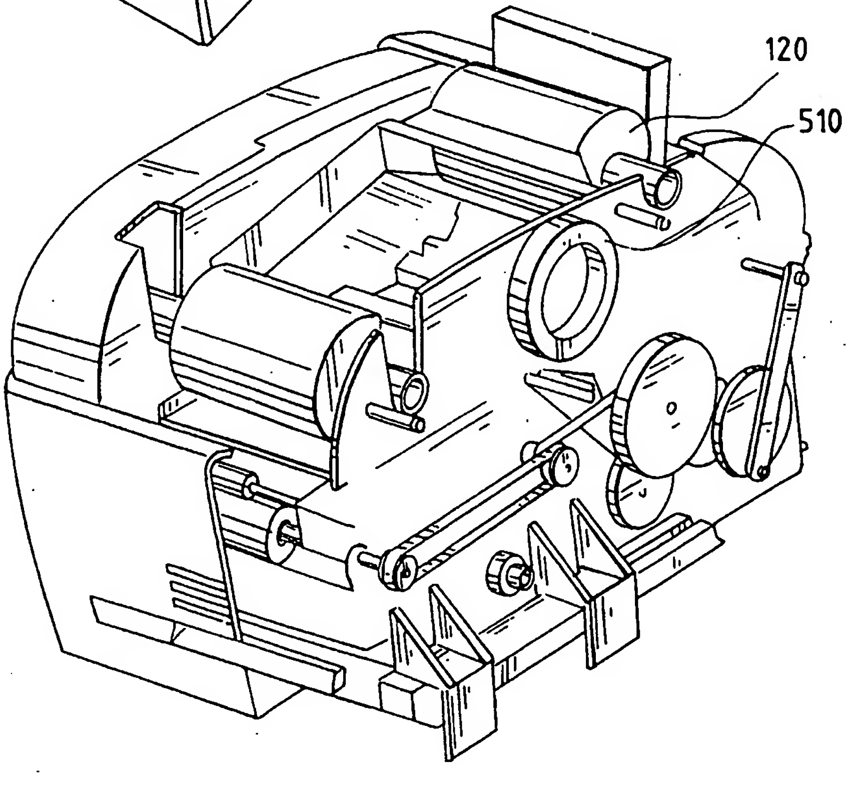


FIG. 7A

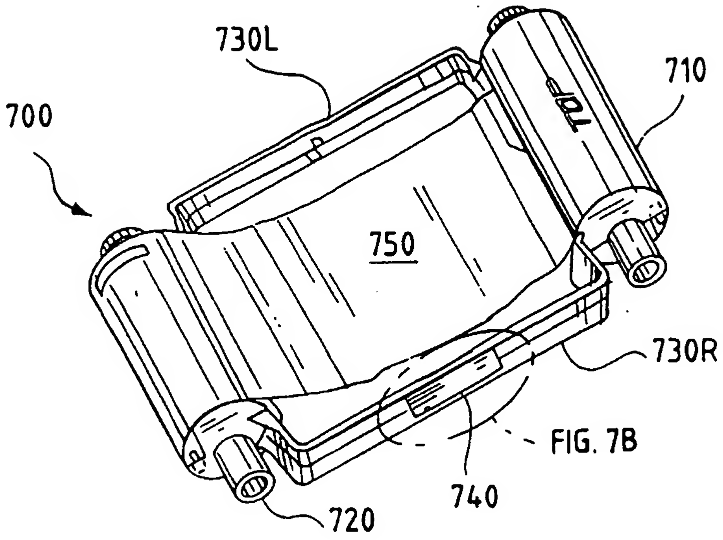


FIG. 7B

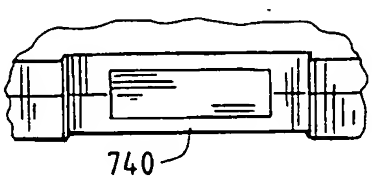


FIG. 7C

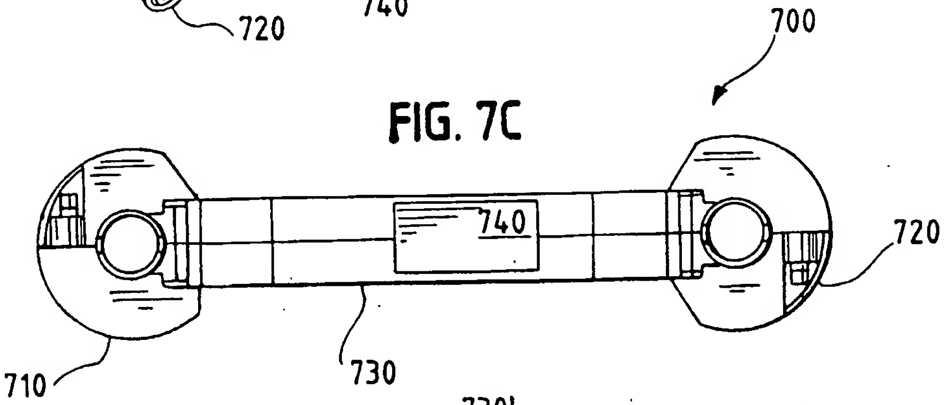


FIG. 7D

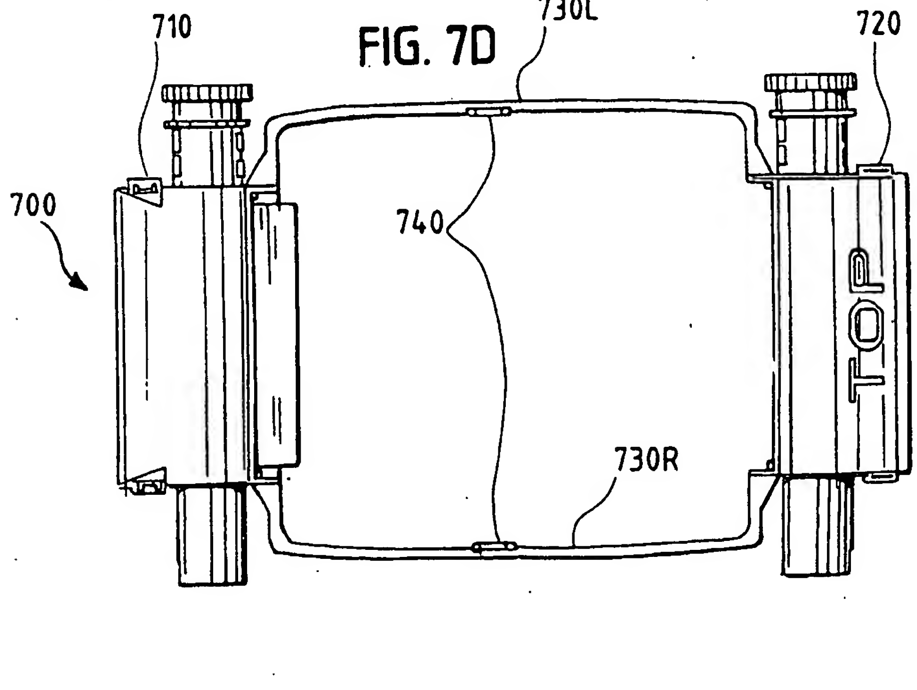


FIG. 8

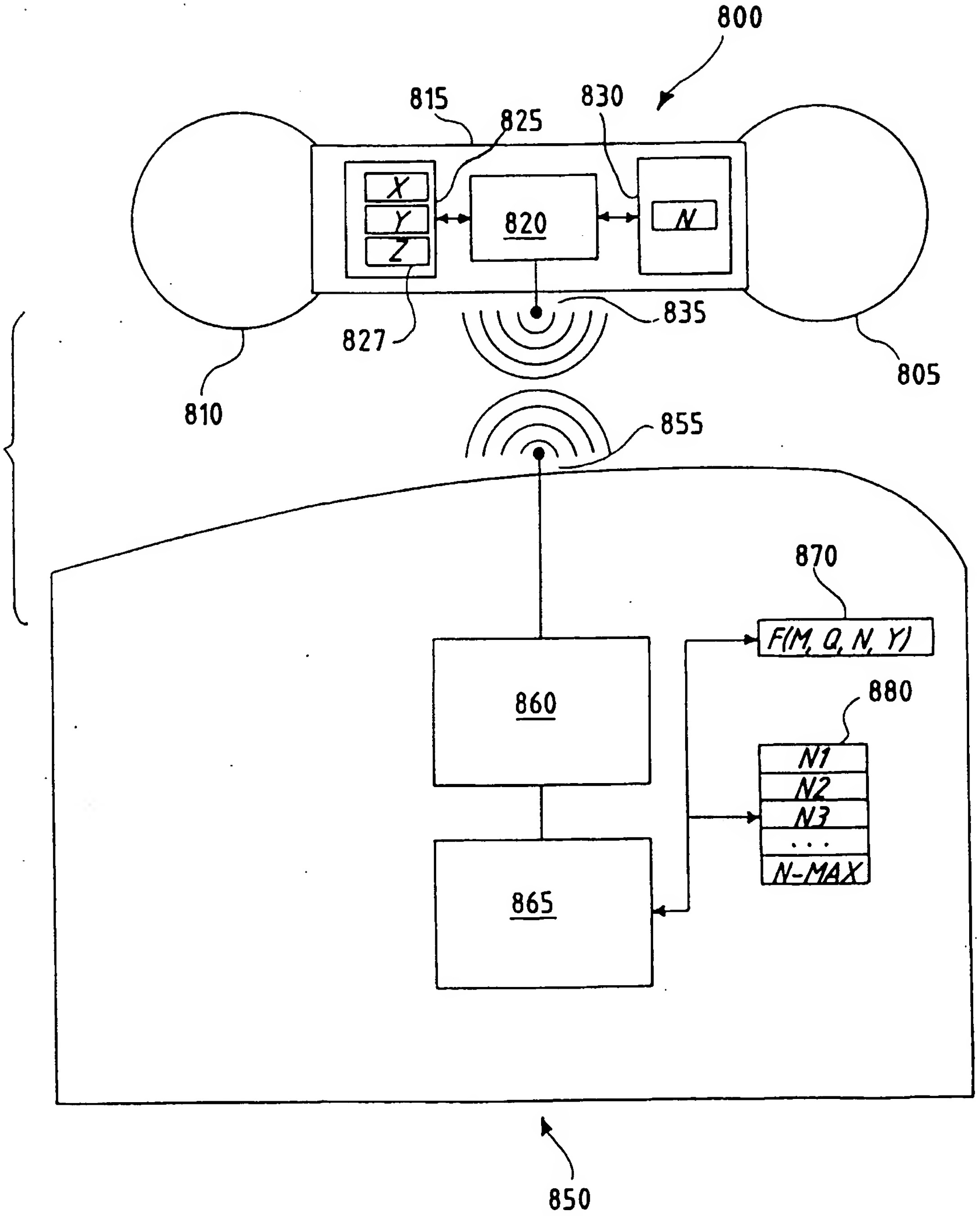

800
815
825
830
X
Y
Z
820
N
835
827
810
805
855
870
F(M, Q, N, Y)
880
860
N1
N2
N3
. . .
N-MAX
865
850

FIG. 9

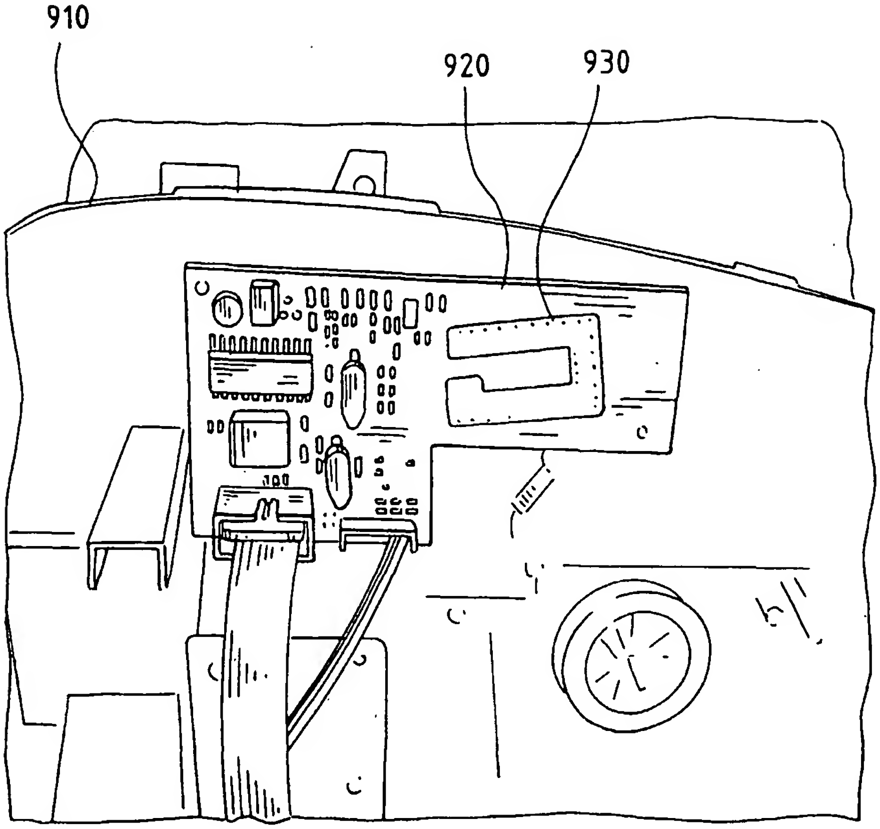


FIG. 10A

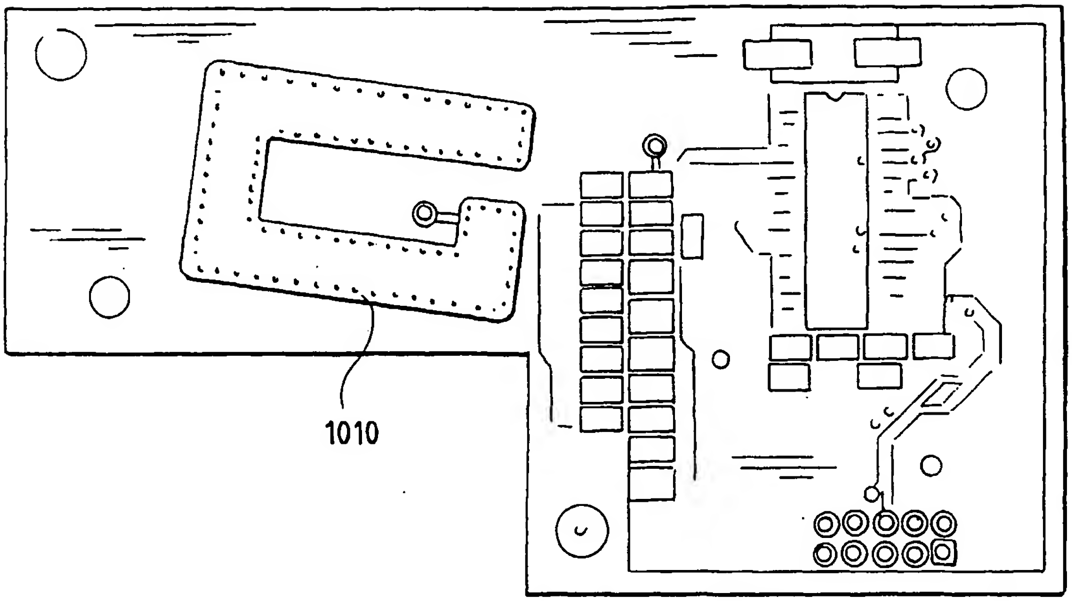


FIG. 10B

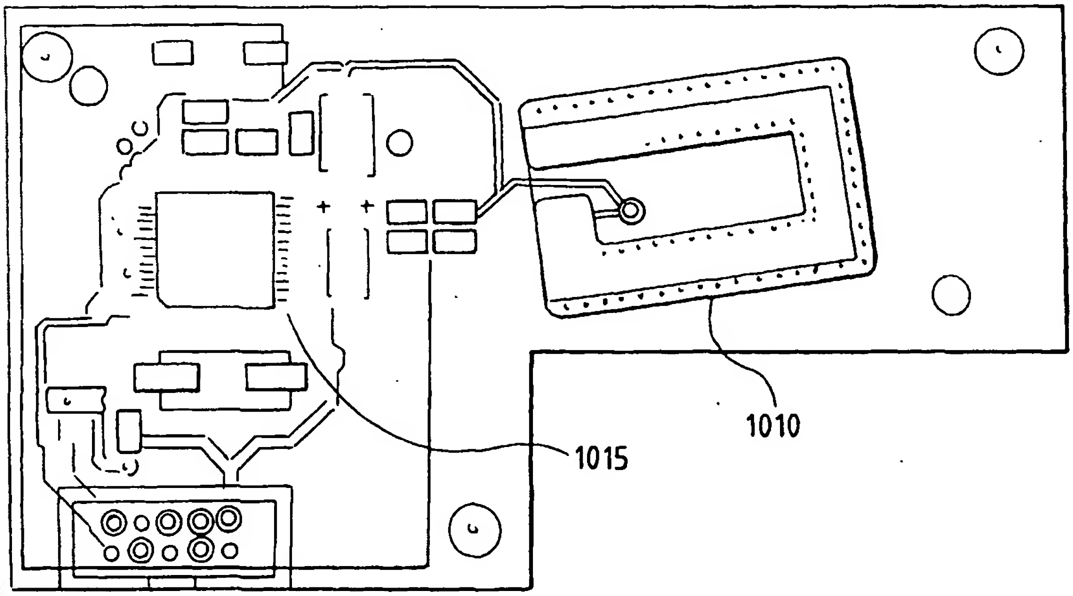


FIG. 11

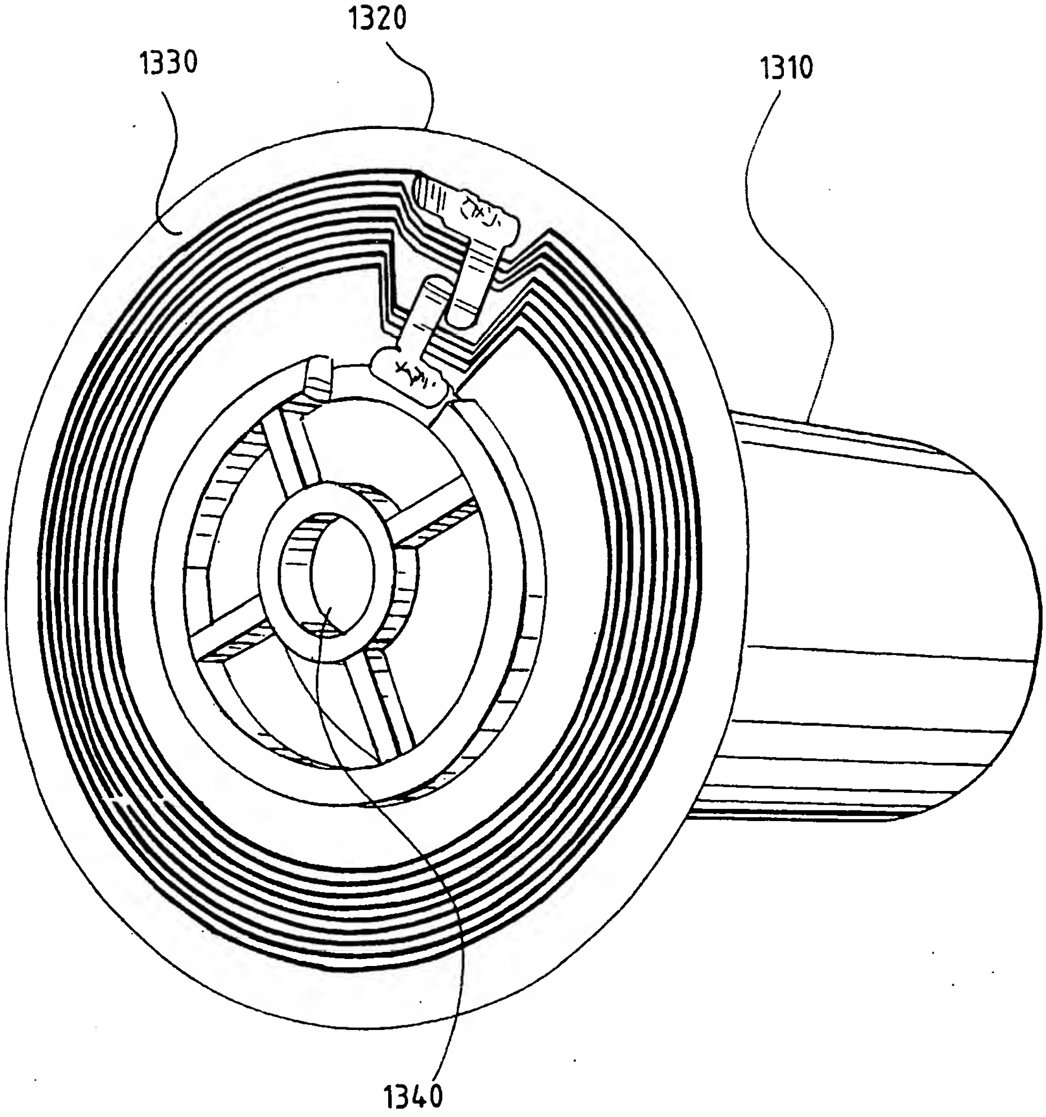


FIG. 12A

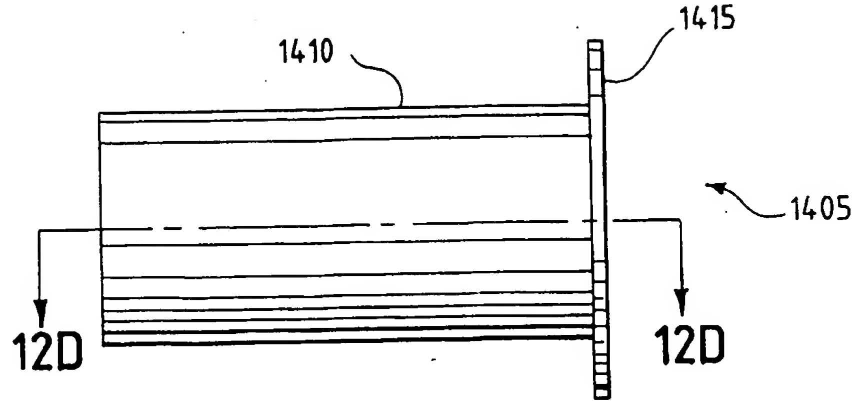


FIG. 12B

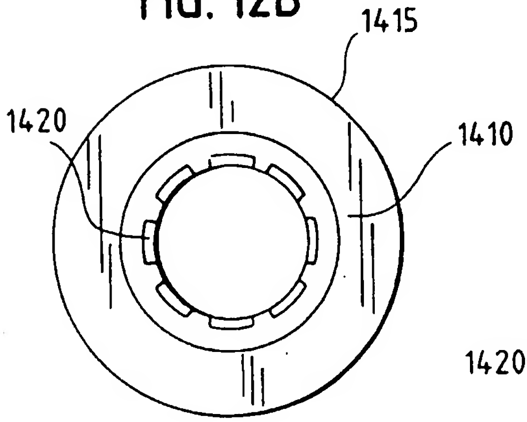


FIG. 12C

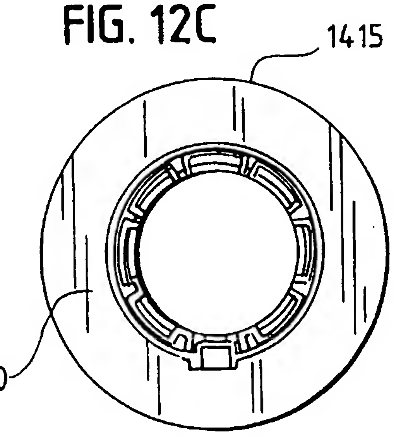


FIG. 12D

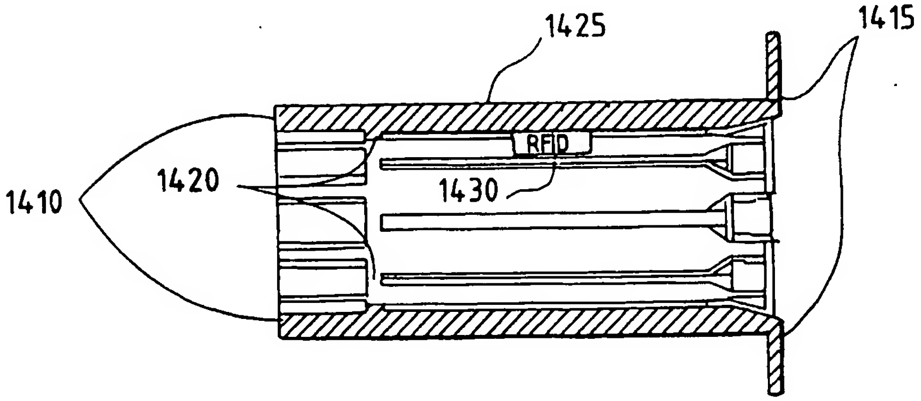
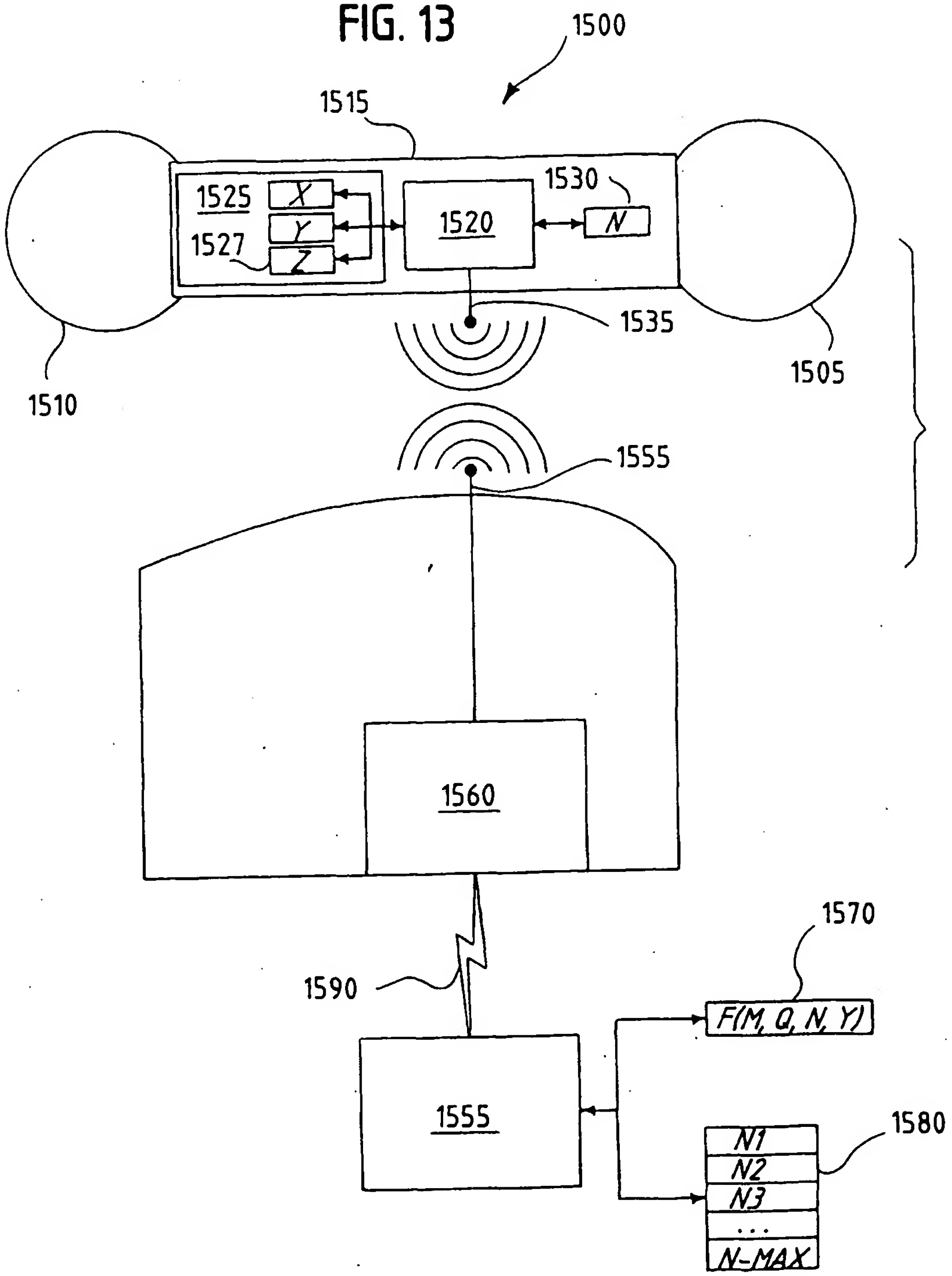


FIG. 13


1500
1515
1525
X
Y
1527
Z
1520
1530
N
1535
1510
1505
1555
1560
1590
1570
F(M, Q, N, Y)
1555
1580
N1
N2
N3
...
N-MAX